Installation and Upgrades

for the

Avaya S8100 Media Server

with the

Avaya G600 and the

Avaya CMC1 Media Gateways

555-233-146
Issue 3
November 2003

Copyright 2003, Avaya Inc.
All Rights Reserved

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: http://www.avaya.com/support. If you are:

- Within the United States, click the *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Management* link. Then click the *International Services* link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

Safety of Information Technology Equipment, IEC 60950, 3rd Edition including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition

Safety Requirements for Customer Equipment, ACA Technical Standard (TS) 001 - 1997

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices operate within the following parameters:

- Maximum power output: -5 dBm to -8 dBm
- Center Wavelength: 1310 nm to 1360 nm

Luokan 1 Laserlaite

Klass 1 Laser Apparat

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposures. Contact your Avaya representative for more laser product information.

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997 and EN55022:1998.

Information Technology Equipment – Immunity Characteristics – Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11
- Powerline Harmonics IEC 61000-3-2
- Voltage Fluctuations and Flicker IEC 61000-3-3

Federal Communications Commission Statement

Part 15:

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Part 68: Answer-Supervision Signaling

Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:

- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For G350 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

For all media gateways:

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

REN is not required for some types of analog or digital facilities.

Means of Connection

Connection of this equipment to the telephone network is shown in the following tables.

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9-BN	6.0F	RJ48C, RJ48M
	04DU9-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

For all media gateways:

If the terminal equipment (for example, the media server or media gateway) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. It is recommended that repairs be performed by Avaya certified technicians.

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Declarations of Conformity

United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at: http://www.part68.org by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC). This equipment has been certified to meet CTR3 Basic Rate Interface (BRI) and CTR4 Primary Rate Interface (PRI) and subsets thereof in CTR12 and CTR13, as applicable.

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

Japan

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya support Web site: http://www.avaya.com/support.

Checklists and job aids

This section contains checklists and job aids for common installation and upgrade procedures. The checklists provide high-level summaries of the procedural steps and cross-reference other sections of this document for additional details. The Job Aids provide the detailed steps to upgrade the S8100 system for three upgrade scenarios.

This section contains the following checklists and job aids:

Checklists

- Initial installation on page 5
- System initialization on page 8
- Administer INTUITY AUDIX digital networking on page 11

Job aids

- Upgrade an S8100's R10+ software using a CD on page 12
- Replace an S8100's hard drive on page 20
- Upgrade an S8100's R9.5 software by replacing the S8100 on page 26

Initial installation

This checklist highlights the high-level tasks for installing and cabling the cabinet to physically connect and access an Avaya S8100 Media Server with an Avaya G600 Media Gateway or a legacy Avaya CMC1 Media Gateway.

	Installation tasks	For more information
1	Verify that every site requirement is met.	See Site requirements on page 58.
2	Confirm that customer's order includes all equipment needed.	For a G600, see Check customer's order on page 59. For a CMC1, see Check customer's order on page 343.
3	Correct shipping errors. — Return defective and over-shipped equipment. Returned: _____ Date: November 2003 _____ — Direct short-shipped reports to National Parts. Report #: _____ Sent to: _____	For a G600, see Correct shipping errors on page 59. or For a CMC1, see Correct shipping errors on page 344.
4	Unpack and inspect equipment using lifting precautions.	For a G600, see Unpack and inspect on page 60. For a CMC1, see Unpack and inspect on page 344.

Installation tasks		For more information
5	For S8100, determine which equipment is required and which is optional.	For a G600, see Comcodes for equipment used with G600 on page 63. For a CMC1, see Comcodes for equipment used with CMC1 on page 346.
6	Install the system's cabinet, making sure there is adequate ventilation. — Verify the carrier address ID on G600 or CMC1 cabinets. ID: _____ — Mount the cabinets. For G600, print a 7 × 11″copy of the G600 mounting template provided on the CD.	For a G600, see Install and cable a G600 cabinet on page 65. or For a CMC1, see Install an S8100 with a CMC1 system cabinet on page 348.
7	Check electrical components. — Check AC power. — Ground power supply. — Connect uninterruptible power supply (UPS). — Disconnect AC power by pulling the AC power cord from the appliance inlet. — Connect cabinet and other grounds. — Install coupled bonding connector. — Connect the power cords.	For a G600, see Check AC power and ground for G600 on page 72. or For a CMC1, see Check AC power and ground for CMC1 on page 357.
8	Connect the cables. — Install the Processor Interface cable. — Install the system cables for multiple cabinets, if necessary.	For a G600, see Cable a G600 system on page 78. or For a CMC1, see Cable a CMC1 system on page 367.
9	Install the S8100 patch panels (G600) or the main distribution frame (CMC1).	For a G600, see Install G600 patch panels and external modem on page 84. or For a CMC1, see Install CMC1 main distribution frame (MDF) and external modem on page 370.
10	Install equipment-room hardware for G600 or CMC1. — Cross-connect the cabinet to the patch panels for G600 or to the MDF for CMC1. — Identify the allowed circuit packs. — Install the circuit packs. — Be sure that off-premises circuits have protection from hazardous voltages and currents. — Install sneak fuse panels. — For CMC1, label the MDF.	See: DEFINITY Communications System Generic 1 and Generic 3 Main Distribution Field Design (555-230-630) ***and*** Install equipment-room hardware for G600 on page 86 or Install equipment-room hardware for CMC1 on page 372.

Installation tasks		For more information
11	Set ringing option.	See Set ringing option for G600 on page 97 or See Set ringing option for CMC1 on page 385.
12	Install and wire telephones and other equipment. — Install attendant console. (optional) — Install 26B1 Console. (optional)	See Install and wire telephones and other equipment on page 99.
13	Connect external alarms and auxiliary connections.	See Connect external alarms and auxiliary connections on page 113.
14	Install the BRI terminating resistor.	See Install the BRI terminating resistor on page 116.
15	Use multipoint adapters to provide signal fanout of the T-interface.	See Install multipoint adapters on page 119.
16	Wire the off-premises stations with the cabling provided by the local telephone company.	See Install off-premises station wiring on page 122.
17	Install the emergency-transfer panel (or equivalent) and associated analog telephones to enable emergency transfer.	See Install emergency-transfer panel and associated telephones on page 127.
18	Connect modem.	See Connect modem to telephone network on page 134 and Connect modem on page 135.
19	Set the neon voltage for S8100/CMC1, only if the ringing option is set to 25 Hz. (There is no need to do this for S8100/G600.)	See Set neon voltage to prevent ring ping on page 136.
20	Finish the installation.	See Complete installation on page 137.

System initialization

This checklist highlights the high-level tasks required to initialize the S8100 Media Server with the G600 or the CMC1 Media Gateways.

Installation tasks		For more information
1	Power up and observe that the TN2314 circuit pack's LEDs light according to a predefined sequence.	See Power up and observe LEDs on page 162.
2	Connect the laptop computer.	See Connect the laptop to S8100 system on page 140.
3	Start a Telnet session.	See Via a Telnet session on page 152.
4	Verify the software's version number with the CD-ROM that shipped with the system. Version #: _____	See Verify the software's version number on page 163.
5	Determine the correct serial number. Serial #: _____	See Determine the serial number on page 163.
If you have the serial # from the order, this step may be completed **prior** to the site visit.		See http://www.avaya.com/services/rfa for instructions on how to use RFA.
6	Download a license using Avaya's Remote Feature Activation (RFA).	
7	Administer customer's LAN parameters: Machine Name, S8100 IP address, DNS and WINS IP address using the setip command.	See Set up customer's LAN parameters on page 163.
8	Reboot the system using **reboot nice**.	See Set up customer's LAN parameters on page 163.
Both of these steps may be completed **prior** to the site visit.		See Obtain the license and password files on page 165.
9	Download a password file.	
10	Download an installation script.	See Obtain the installation script file on page 166.
11	Use FTP to transfer files to server and install the license, password, and installation script files.	See Install the password file, license file, and installation scripts on page 168.
12	Test alarming on the S8100.	See Test alarm call out on page 172.
13	Resolve any alarms.	See *Maintenance for the Avaya S8100 Media Server with the Avaya G600 Media Gateway* and *the Avaya CMC1 Media Gateway* (555-233-149).
14	Check system's status using bash commands.	See Avaya (Lucent) access controller bash commands on page 329.

Installation tasks		For more information
15	Enable customer's logins. — INTUITY AUDIX logins — Web logins — S8100 logins	See: Enable INTUITY AUDIX logins on page 174. Enable customer's web logins on page 174. Set up login accounts on page 290. Windows logins for customers on page 286. Communication Manager logins for customers on page 291.
16	Administer S8100. **CAUTION:** The S8100 is preconfigured to be a member of a local Workgroup and should not be made a member of a customer's Windows domain. If this is done, connectivity with Avaya Services will not operate correctly because user account authentication will no longer be done by the S8100. To check for proper workgroup membership, on the S8100 Windows desktop right-click the My Computer icon (this may have another name if the customer has changed it) and select Properties. Then choose the Network Identification tab to view the workgroup information. — Use Windows 2000 to set the time zone. — Use Windows 2000 to set the system date and time. — Administer customer's LAN interface. — Set up country-specific call-progress tones. — Enable or disable SNMP. — Set country options on the change system parameters country options screen. — Set up your systems. — Add translations. — Administer telephone features per customer's order. — Set up call-detail recording (CDR).	See Administer S8100 on page 174.
17	Set up an Avaya-provided call-accounting product. — Telecommunications Management System (TMS). — Call Accounting System (CAS).	See Call accounting on page 185.

Installation tasks		For more information
18	Initialize Communication Manager for INTUITY AUDIX. — Check the dial plan. — Check hunt groups. — Check class of service. — Check class of restriction. — Change the dial plan. — Add extension ranges. — Add stations. — Make a hunt group. — Change coverage path. — Add test phones.	See Administer Communication Manager for INTUITY AUDIX initialization on page 185. For information about INTUITY AUDIX commands and initializing INTUITY AUDIX, see INTUITY AUDIX administration on page 194.
19	Place test calls to verify that the dial tone, ringing pattern, and talk path are acceptable.	See Place a test call on page 182.
20	Install Message Manager.	See Message Manager on page 257.
21	Administer the SNMP agent. — Configure SNMP trap destinations. — Configure SNMP community strings. — Start and stop SNMP using a bash command or the Web interface.	See Administer SNMP on page 199.
22	Schedule backups to prevent loss of data.	See Schedule backups on page 205.

Administer INTUITY AUDIX digital networking

This checklist highlights the high-level tasks required to administer INTUITY AUDIX digital networking after the S8100 system's initial administration is finished.

Installation tasks		For more information
1	Perform initial administration. — Be sure you have design center specifications for TCP/IP, network channels, the local machine, and every remote machine.	See Initial administration tasks on page 207.
2	View the Feature Options window to see the purchased options for digital networking.	See View the Feature Options window on page 209.
3	Change the number of administered remote users to be ≥ the number of mailboxes on every remote system networked with this local system.	See Change number of administered remote users on page 210.
4	Enable the network channels so that the local INTUITY AUDIX system can exchange voice messages over the digital network.	See Administer networking channels on page 211.
5	You can change local machine's information on the Machine Profile screen and on the Local Machine Administration window. (If you do, inform every remote network administrator about the changes.) — Change the local machine profile. — Complete the Local Machine Administration window. — Add a remote machine, if you want users to be able to exchange message with INTUITY AUDIX users on another machine. — Complete the Digital Machine Administration window (via Web browser) to enter information for connecting to the remote machine. — Use the Machine Profile screen to enter networking information required for each remote machine. — Perform a full remote update, if necessary. — Reset automatic deletion of non administered remote users to conserve server space. — View remote extensions to verify that the local machine database updated the remote subscriber information.	See Change local machine's information on page 212.

Upgrade an S8100's R10+ software using a CD

This Job Aid provides the steps for upgrading an S8100 Media Server's software by transferring the new software from a CD. This procedure applies to either a full- or a dot-release upgrade.

Access keys

The access method for each step is identified by the following keys:

LT	Technician's laptop
LT-IE	Internet Explorer/Web interface on the laptop
SDT	S8100's Windows desktop
SDT-IE	Internet Explorer/Web Interface on the S8100's Windows desktop (Note that SDT and SDT-IE are opened inside of LT-IE.)
BS	Bash shell on S8100's Windows desktop
LAC	LAC shell
SAT	System-administration terminal
{...}	Information in braces is for Windows 2000

Upgrade steps

Step		Details	
1	For a direct connection between the technician's laptop and the S8100's service port: **LT** – Change the laptop's IP address to 192.11.13.5	**a**	Right-click the 'Network Neighborhood' {My Network Places} icon on the laptop's desktop, and select Properties.
		b	{Right-click 'PCMIA Ethernet Connection' (or Local Area Connection), and select Properties.}
		c	Highlight the TCP/IP icon from the popup window, and select Properties. Check the 'Specify an IP address' {'Use the following IP address'} radio button.
		d	Enter **192.11.13.5** in the IP address field and **255.255.255.252** in the subnet mask field, and click OK to close the popup windows.
2	**LT-IE** – Disable proxy servers on Internet Explorer.	**a**	Open Internet Explorer and select Tools, Internet Options, the Connections tab, and LAN Settings.
		b	Uncheck the 'Use a proxy server' radio button and click OK to close the popup windows.
3	Connect the laptop to the service jack on the front of the S8100's Processor board.	**a**	Connect a cable from the laptop's PCMCIA Ethernet card to an RJ45 coupler.
		b	Connect a cross-over (flip) cable from the coupler to the TN2314's RJ45 jack.
4	**LT-IE** – Connect to the S8100 server via the web interface.	Open Internet Explorer on the laptop, and enter **192.11.13.6** in the URL address bar to connect to the processor.	
5	**LT-IE** – Open the S8100's desktop. **Note:** Terminal server client and terminal services Active X must be installed on the laptop. The easiest way to do this is to upgrade your Windows 95 laptop's browser to Internet Explorer version 5.5 or higher.	**a**	Click 'Administer System' and log in using **lucent3** for login and password. A domain is not required. Select 'continue' at license agreement window.
		b	Select 'Login to 192' under Remote Control – Terminal Services.
		c	If a VBScript error message appears, click OK.
		d	Click the Connect button (leave the Server field blank).
		e	If a VBScript message appears, click OK (you can resize the Terminal Services screen to full size by pressing ctlr-alt-Pause). A log-in window opens.
		f	Log in using **lucent3**. After logging in, the S8100's Windows 2000 desktop is displayed.
6	**SDT** – Open a bash shell window.	Click **Start** → **Run** → **bash**.	
7	**BS** – Open a LAC window.	Execute **telnet 127.1**.and log in using **lucent3**.	

Step		Details
8	**LAC** – Open a SAT window and save translations.	**a** Type **multivantage** to open a SAT window. (The terminal type is W2KTT.) **b** Run **save translations**.
9	**LAC** – Return to the bash window.	**a** Type **logoff** to log out of the SAT window. **b** Press Enter and type **exit** to exit the LAC window. **c** Close the LAC window. **Note:** Do not close the LAC window until you have issued the 'exit' command.
10	**SDT** – Open Internet Explorer on the S8100's desktop and log in using **lucent3**.	**Note:** This step could be done by closing the S8100's desktop and using the laptop's IE session, but then you would need to set up a new S8100-desktop session for subsequent steps.
11	**SDT-IE** – Backup everything to the PCMCIA card or to a network location. **Note:** If the medium you are backing up to runs out of space, a message will appear noting the files that were not backed up. In this case, find a different backup location or PCMCIA card with enough capacity and rerun the entire backup.	**a** Click 'Administer System'. **b** Log in with **lucent3**. **c** Click 'Backup & Restore' under System Maintenance. **d** Click 'Immediate Backup'. **e** Under "Choose Items for Immediate Backup," select everything that is installed. **Note:** If the S8100's internal AUDIX is being used, you must do two backups. First, select the "AUDIX translations, names & messages" radio button in addition to "MultiVantage announcements" and "MultiVantage translations." When the backup finishes, return to the 'Immediate Backup' screen and select only the "AUDIX announcements" radio button and send this backup to the same or a different location. **f** Set Destination to PCMCIA or click 'Other Location' to send the backup to a network location. **g** Click the Backup button.
12	**SDT-IE** – Record AUDIX extension length. **Note:** You will need to verify the extension length later.	**a** Click the Back icon (on the IE tool bar) twice to return to the Administer System page. **b** From the explorer window, click 'Default AUDIX Settings'. **c** Note whether AUDIX is enabled. If so, click 'AUDIX Extension Length' and record the extension length.
13	**SDT-IE** – Close Internet Explorer on the S8100's desktop.	
14	**SDT** – Open a bash shell window (if not already open).	On the S8100's desktop, click **Start** → **Run** → **bash**.

Step		Details
15	**BS** – **Important! –** Display and record the customer's network and product information.	**a** From the bash shell, execute the following three commands – **setip**, **productid**, **oss**. **b** ***Write down all of this information exactly as it appears on the screen.*** You will need to re-enter this information later.
16	**BS** – Close the bash window.	Type **exit**.
17	**SDT** – Connect to and open the laptop's CD-ROM drive from the S8100 server. **Note:** Make sure the CD-ROM drive on the laptop is shared. For more detaied information, see: • Connectivity and access to an S8100 system on page 139 • Map CD-ROM for an S8100 upgrade on page 339	**a** On the S8100's desktop, right-click My Network Places, and select Search. **b** When the search window pops up, click Computers in the "Search for other items" list. **c** Enter the IP address for the laptop (typically, 192.11.13.5) in the Computer Name window, and click the Search Now button. **d** Double-click the computer icon when it appears in the Name list in the right panel. **e** If a Connect As window appears, enter the user name (in the Connect as window) and password that you normally use to log onto your laptop. Precede your user name with the domain name\; i.e., <domain name>\<user name> The list of shared devices on your laptop should appear. **f** Double-click the CD-ROM drive to display its contents, including setup.exe.

Step		Details
18	**SDT** – If the S8100 system is running Windows 2000 with Service Pack 2 or 3, you need to upgrade to Service Pack 4 (SP4). You can obtain the SP4 upgrade from either the: • Avaya software CD-ROM • Microsoft website	**a** Check the Windows service pack's version: — On the S8100's Windows desktop, right-click the My Computer icon. — Click Properties and check the service pack's version. — If running SP4, skip to Step 23. If running either SP2 or SP3, continue with this step to upgrade to SP4. Upgrade to SP4: **b** From the bash shell, execute **shutdown all**. **c** Browse the contents of the CD-ROM (which you connected to in Step 17). In the folder, "Windows Updates," find the SP4 upgrade file, ***W2Ksp4.exe***, and double-click it. **d** When the option for archiving files comes up, choose "**Do not archive files**." Accept the other defaults. **e** If an option to restart Windows 2000 appears when the upgrade to SP4 finishes, choose **no** to decline. **f** From the bash shell do a manual reboot, by executing **start all**.
19	If you upgraded to SP4 in Step 18, and restarted Windows 2000, you will need to repeat Step 4 and Step 5 to get back to the S8100's Windows desktop.	
20	**SDT** – Open a bash shell window.	On the S8100's desktop, click **Start** → **Run** → **bash**.
21	**BS** – Shutdown every application.	From the bash shell, execute **shutdown all**.
22	**BS** – Close the bash window.	Type **exit**.
23	**WARNING:** Execute this step from the S8100's Windows desktop, ***not*** from the laptop's desktop. Running setup on the laptop will overwrite the contents of the laptop's hard drive. **SDT** – Upgrade the S8100's system software.	Browse the contents of the CD-ROM (which you connected to in Step 17). Find and double-click **setup.exe**, and follow the Wizard's steps for the upgrade.
24	**SDT** – After the upgrade finishes, if the bash shell is still open, the platform should reboot on its own. If the bash shell is not open, open it and execute **reboot nice** to restart the system.	
25	Wait approximately 5 minutes then reconnect to the S8100's desktop.	Repeat steps **4** through **5**.

Step		Details
26	**SDT** – On the S8100's desktop, double-click the time display and set the *time*, *time zone*, *date*, and *Daylight Savings*.	The time display is in the tool tray at the lower right of the desktop.
27	**SDT** – Disable modem compression.	**a** Click **Start** → **Settings** → **Control Panel**. **b** Double-click Phone and Modem Options. **c** Click the Modems tab. **d** Select the installed modem and click Properties. **e** Click the Advanced tab. **f** Click Change the Default Preferences. **g** In the Compression drop-down list, select Disabled. **h** Close each dialog by clicking **OK**, and close the Control Panel window.
28	**SDT** – Open a bash shell window.	Click **Start** → **Run** → **bash**.
29	**BS** – Verify the software's version.	Type **swversion**. Ensure that the Release number and MultiVantage version number are as expected.
30	**BS** – Verify the customer's parameters that you wrote down in Step 15, using the setip command.	Type **setip** to display the customer's parameters. If any parameter is not as you recorded in Step 15, use the following setip commands to reset those parameters. setip name=<args> setip cust=<args> setip dns=<args> setip wins=<args> setip ras=<args> Replace each "<args>" with the corresponding parameter you recorded in Step 15.
31	**BS** – Administer the product ID and OSS parameters using the 'productid' and 'oss' commands.	**productid multivantage-product-id <arg>** **productid audix-product-id <arg>** **oss <telno> <retries> <retry_interval>** Replace each "<arg>" with the corresponding parameter you recorded from Step 15. For the **oss** command, enter the **<telno>**, **<retries>**, and **<retry_interval>** parameters separated by spaces; do not enter commas.
32	**BS** – Open a LAC window.	Execute **telnet 127.1**, and log on using **lucent3**.
33	**LAC** – Open a bash shell window.	Type **bash**.
34	**BS** – Check license status. If `License-Normal Mode` is displayed, skip Step 35.	Type **statuslicense**.
35	**LAC** – Install the new license and password file from the LAC window using the lucent3 log-in ID.	For details, see Chapter 3 in *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and the Avaya CMC1 Media Gateways, 555-233-146.*

Step		Details
36	**LAC** – Close the LAC window and bash shell.	**a** Type **exit**, and close the telnet window. **b** Type **exit** to close the bash window.
37	**SDT** – Open Internet Explorer on the S8100's desktop and log in.	**a** Double-click the IE icon on the S8100's desktop. **b** Click 'Administer System'. **c** Log in using **lucent3**. **d** Click Continue on the Notice page.
38	**SDT-IE** – Restore the translations and other backed-up data to the hard drive.	**a** Click 'Administer System.' **b** Click 'Backup & Restore.' **c** Click 'Restore.' **d** Select the Source for the restore – The Destination or Other location you entered for the backup in Step 12. **e** Click the **Continue** button. Under "These items will be restored from ... ", every item that was backed up to the location specified in Step d will be selected. **f** Click the **Restore** button. **Note:** If you backed up AUDIX announcements in Step 12, you must do two restores. After the first restore, repeat the steps above using the location of the backed up AUDIX announcements for the Source in Step d.
39	**SDT-IE** – Close Internet Explorer.	
40	**SDT** – Open a bash shell window.	Click **Start** → **Run** → **bash**.
41	**BS** – Shutdown every application.	Execute **shutdown all**.
42	**BS** – After the shutdown finishes, restart every application.	Execute **start all**.
43	**BS** – Monitor the startup's progress.	Execute **statapp**.
44	Verify that call processing comes into service.	
45	Verify that voice messaging comes into service.	
46	**BS** – Telnet into the LAC window from the bash.	Execute **telnet 127.1**, and log in using **lucent3**.
47	**LAC** – Open a SAT window.	Type **multivantage** to open a SAT window. (The terminal type is W2KTT.)
48	**SAT** – Verify that there is no translation corruption.	If there are corrupted translations, a message will appear when the SAT window opens.
49	**SAT** – Verify no-license/emergency numbers.	Type **change system-parameters features**. See ''Administer No-License/Emergency Numbers'' in *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and the Avaya CMC1 Media Gateways, 555-233-146.*

Step		Details
50	**SAT** – Verify that no major or minor alarms are present.	Type **display alarms**.
51	**SAT** – Verify outgoing alarm reports link to INADS.	Type **test inads-link**.
52	**SAT** – Save translations.	Type **save trans**.
53	**SAT** – Log out of SAT, and exit LAC.	**a** Type **logoff**, and respond with **y** to close the SAT session. **b** Type **bash** to go to the bash shell.
54	**BS** – Verify Intuity alarms.	Type **logsend -tTST**.
55	**BS** – Verify GAM alarms.	Type **wrntevent GAM 0 9991**. **Note:** This causes a Major GAM alarm. After the system has called out, enter **cleargamalarm all** at the **BASH prompt** to retire the alarm. This alarm also generates a Maestro case that the INADS group will need to close.
56	**BS** – Close the bash windows.	**a** Type **exit** to close the bash window. **b** Type **exit** to close the LAC window.
57	**LT-IE** – Backup the translations and other data to the PCMCIA card or to a network location.	**a** Click 'Administer System'. **b** Click 'Backup & Restore' under System Maintenance. **c** Click 'Immediate Backup'. **d** Under "Choose Items for Immediate Backup," select everything that is installed. **e** Set Destination to PCMCIA, or click 'Other Location' to backup to a network location. **f** Click the Backup button. **Note:** If the medium you are backing up to runs out of space, a message will appear noting the files that didn't get backed up.
58	Close Internet Explorer on the S8100's desktop and on the laptop.	
	SECURITY ALERT: When you are finished with the upgrade procedures, you should restore your laptop to its original configuration, including unsharing the CD drive. When connected to a network, a shared drive is a potential security risk.	

Replace an S8100's hard drive

This Job Aid provides the steps for replacing the hard drive on the S8100 Media Server (TN2314) circuit pack. The media server's software release on the new hard drive may be the same as, or later than, the software release on the hard drive to be replaced. If the media server's software release on the new hard drive is earlier than the software release on the hard drive to be replaced, you must upgrade the software on the new hard drive after the replacement.

Access keys

The access method for each step is identified by the following keys:

LT	Technician's laptop
LT-IE	Internet Explorer / Web interface on the laptop
SDT	S8100's Windows desktop
SDT-IE	Internet Explorer/Web interface on the S8100's Windows desktop (Note that SDT and SDT-IE are opened inside of LT-IE.)
BS	Bash shell on S8100's Windows desktop
LAC	LAC shell
SAT	System-administration terminal
{...}	Information in braces is for Windows 2000

Upgrade steps

Step		Details	
1	For a direct connection between the technician's laptop and the S8100's service port. **LT** – Change the laptop's IP address to 192.11.13.5	**a**	Right-click the 'Network Neighborhood' {My Network Places} icon on the laptop's desktop and select Properties.
		b	{Right-click 'PCMIA Ethernet Connection' (or Local Area Connection) and select Properties.}
		c	Highlight the TCP/IP icon from the popup window and select Properties. Check the 'Specify an IP address' {'Use the following IP address'} radio button.
		d	Enter **192.11.13.5** in the IP address field and **255.255.255.252** in the subnet mask field and click OK to close the popup windows.

Step		Details	
2	**LT-IE** – Disable proxy servers on Internet Explorer.	**a**	Open Internet Explorer and select Tools, Internet Options, the Connections tab, and LAN Settings.
		b	Uncheck the 'Use a proxy server' radio button and click OK to close the popup windows.
3	Connect the laptop to the service jack on the front of the S8100's Processor board.	**a**	Connect a cable from the laptop's PCMCIA Ethernet card to an RJ45 coupler.
		b	Connect a cross-over (flip) cable from the coupler to the TN2314's RJ45 jack.
4	**LT-IE** – Connect to the S8100 server via the web interface.	Open Internet Explorer on the laptop and enter **192.11.13.6** in the URL address bar to connect to the processor.	
5	**LT-IE** – Open the S8100's desktop. **Note:** Terminal server client and terminal services Active X must be installed on the laptop. The easiest way to do this is to upgrade your Windows 95 laptop's browser to Internet Explorer 5.5.	**a**	Click 'Administer System' and log in using **lucent3** for log-in ID and password. A domain is not required. Select 'continue' at license agreement window.
		b	Select 'Login to 192' under Remote Control – Terminal Services.
		c	If a VBScript error message appears, click OK.
		d	Click the Connect button (leave the Server field blank).
		e	If a VBScript message appears, click OK (you can resize the Terminal Services screen to full size by pressing ctlr-alt-Pause). A log-in window will open.
		f	Log in using **lucent3**. After logging in, the S8100's Windows 2000 desktop is displayed.
6	**SDT** – Open a bash shell window.	Click **Start** → **Run** → **bash**.	
7	**BS** – Open a LAC window.	Execute **telnet 127.1**,.and log in using **lucent3**.	
8	**LAC** – Open a SAT window and execute **save translations**.	Type **multivantage** to open a SAT window. (The terminal type is W2KTT.)	
9	**LAC** – Return to the bash window.	**a**	Type **logoff** to log out of the SAT window.
		b	Press Enter, and type **exit** to exit the LAC window.
		c	Close the LAC window.
		Note: Do not close the LAC window until you have issued the 'exit' command.	
10	**SDT** – Open Internet Explorer on the S8100's desktop and log in using **lucent3**.	**Note:** This step could be done by closing the S8100's desktop and using the laptop's IE session, but then you would need to set up a new S8100-desktop session for the subsequent steps.	

Step		Details
11	**SDT-IE** – Backup everything to the PCMCIA card or to a network location. **Note:** If the medium you are backing up to runs out of space, a message will appear noting the files that were not backed up. In this case, find a different backup location or PCMCIA card with enough capacity and rerun the entire backup.	**a** Click 'Administer System' **b** Log in with **lucent3**. **c** Click 'Backup & Restore' under System Maintenance. **d** Click 'Immediate Backup'. **e** Under "Choose Items for Immediate Backup," select everything that is installed. **Note:** If the S8100's internal AUDIX is being used, you must do two backups. First, select the "AUDIX translations, names & messages" radio button in addition to "MultiVantage announcements" and "MultiVantage translations." When the backup finishes, return to the 'Immediate Backup' screen and select only the "AUDIX announcements" radio button and send this backup to the same or a different location. **f** Set Destination to PCMCIA or click 'Other Location' to send the backup to a network location **g** Click the Backup button.
12	**SDT-IE** – Record AUDIX extension length. **Note:** You will need to verify the extension length later.	**a** Click the Back icon (on the IE tool bar) twice to return to the Administer System page. **b** From the explorer window, click 'Default AUDIX Settings'. **c** Note whether AUDIX is enabled. If so, click 'AUDIX Extension Length' and record the extension length.
13	**SDT-IE** – Close Internet Explorer on the S8100's desktop.	
14	**SDT** – Open a bash shell window (if not already open).	Click **Start** → **Run** → **bash**.
15	**BS** – **Important!** – Display and record the customer's network and product information.	**a** From the bash shell, execute the following three commands – **setip**, **productid**, **oss**. **b** ***Write down all of this information exactly as it appears on the screen.*** You will need to re-enter this information later.
16	**BS** – From the bash shell, execute **shutdown system**.	
17	The green "Complete" LED on the S8100's faceplate will be flashing during the shutdown process. Wait until this LED is on steady. Then power down the system.	
18	Disconnect the cross-over cable from the Processor board and remove the board from the cabinet.	

Step		Details
19	Carefully replace the hard drive on the Processor board with the new hard drive.	**Note:** Hard drives are always installed in the top slot of the drive bay.
20	Re-install the Processor board into the platform and power up the system.	
21	Wait approximately 5 minutes then reconnect to the S8100's desktop and open a bash shell.	Repeat steps **3** through **5**.
22	**BS** – Verify the software's version.	Type **swversion**. Ensure that the Release number and MultiVantage version number are as expected.
23	**SDT** – On the S8100's desktop, double-click the time display and set the *time*, *time zone*, *date*, and *Daylight Savings*.	The time display is in the tool tray at the lower right of the desktop.
24	**SDT** – Disable modem compression.	**a** Click **Start** → **Settings** → **Control Panel**. **b** Double-click Phone and Modem Options. **c** Click the Modems tab. **d** Select the installed modem and click Properties. **e** Click the Advanced tab. **f** Click Change the Default Preferences. **g** In the Compression drop-down list, select Disabled. **h** Close each dialog by clicking **OK**, and close the Control Panel window.
25	**SDT** – Open a bash shell window.	Click **Start** → **Run** → **bash**.
26	**BS** – Administer the customer's parameters that you wrote down in Step 15, using the setip command.	**setip name=<args>** **setip cust=<args>** **setip dns=<args>** **setip wins=<args>** **setip ras=<args>** Replace each "<args>" with the corresponding parameter you recorded in Step 15.
27	**BS** – Administer the product ID and OSS parameters using the 'productid' and 'oss' commands.	**productid multivantage-product-id <arg>** **productid audix-product-id <arg>** **oss <telno> <retries> <retry_interval>** Replace each "<arg>" with the corresponding parameter you recorded from Step 15. For the **oss** command, enter the **<telno>**, **<retries>**, and **<retry_interval>** parameters separated by spaces; do not enter commas.
28	**BS** – Telnet into the LAC window from the bash.	Execute **telnet 127.1**, and log in using **lucent3.**
29	**LAC** – Install the new license and password file from the LAC window using the lucent3 login ID.	For details, see Chapter 3 in *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and the Avaya CMC1 Media Gateways, 555-233-146.*

Step		Details	
30	**LAC** – Exit the LAC window and bash shell.	**a**	Type **exit**, and close the telnet window.
		b	Type **exit** to close the bash window.
31	**SDT** – Open Internet Explorer on the S8100's desktop and log in.	**a**	Double-click the IE icon on the S8100's desktop.
		b	Click 'Administer System'.
		c	Login using **lucent3**.
		d	Click Continue on the Notice page.
32	**SDT-IE** – Restore the translations and other backed-up data to the hard drive. **Note:** The Windows logins of **vm**, **sa**, **browse**, and **NTadmin** are reset to their factory defaults. The customer should reset these passwords and reinstall other Windows accounts they may have created.	**a**	Click 'Administer System.'
		b	Click 'Backup & Restore.'
		c	Click 'Restore.'
		d	Select the Source for the restore – The Destination or Other location you entered for the backup in Step 12.
		e	Click the **Continue** button. Under "These items will be restored from ... ", every item that was backed up to the location specified in Step d will be selected.
		f	Click the **Restore** button.
		Note: If you backed up AUDIX announcements in Step 12, you must do two restores. After the first restore, repeat the steps above using the location of the backed up AUDIX announcements for the Source in Step d.	
33	**SDT-IE** – Close Internet Explorer.		
34	**SDT** – Open a bash shell.	Click **Start** → **Run** → **bash**.	
35	**BS** – Shutdown every application.	Execute **shutdown all**.	
36	**BS** – After the shutdown finishes, restart every application.	Execute **start all**.	
37	**BS** – Monitor the startup's progress.	Execute **statapp**.	
38	Verify that call processing comes into service.		
39	Verify that voice messaging comes into service.		
40	**BS** – Telnet into the LAC window from the bash.	Execute **telnet 127.1** and logon using **lucent3**.	
41	**LAC** – Open a SAT window.	Type **multivantage** to open a SAT window. (The terminal type is W2KTT.)	
42	**SAT** – Verify that there is no translation corruption.	If there are corrupted translations, a message will appear when the SAT window opens.	
43	**SAT** – Verify that no major or minor alarms are present.	Run **display alarms**.	
44	**SAT** – Verify outgoing alarm reports link to INADS.	Run **test inads-link**.	

Step		Details
45	**SAT** – Verify no-license/emergency numbers.	Type **change system-parameters features**. See ''Administer No-License/Emergency Numbers'' in *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and the Avaya CMC1 Media Gateways, 555-233-146.*
46	**SAT** – Save translations.	Run **save trans**.
47	**SAT** – Logoff SAT and exit LAC.	**a** Type **logoff** and respond with **y** to close the SAT session. **b** Type **bash** to go to the bash shell.
48	**BS** – Verify Intuity alarms.	Type **logsend -tTST**.
49	**BS** – Verify GAM alarms.	Type **wrntevent GAM 0 9991**. **Note:** This causes a Major GAM alarm. After the system has called out, enter **cleargamalarm all** at the **BASH prompt** to retire the alarm. This alarm also generates a Maestro case that the INADS group will need to close.
50	**BS** – Close the bash windows.	**a** Type **exit** to close the bash window. **b** Type **exit** to close the LAC window.
51	**LT-IE** – Backup the translations and other data to the PCMCIA card or to a network location.	**a** Click 'Administer System'. **b** Click 'Backup & Restore' under System Maintenance. **c** Click 'Immediate Backup'. **d** Under "Choose Items for Immediate Backup," select everything that is installed. **e** Set Destination to PCMCIA, or click 'Other Location' to backup to a network location. **f** Click the Backup button. **Note:** If the medium you are backing up to runs out of space, a message will appear noting the files that didn't get backed up.
52	Close Internet Explorer on the S8100's desktop and on the laptop.	
	SECURITY ALERT: When you are finished with the upgrade procedures, you should restore your laptop to its original configuration.	

Upgrade an S8100's R9.5 software by replacing the S8100

This Job Aid provides the steps for upgrading an R9.5 DEFINITY ONE or IP600 system to an S8100 system with the current release of Communication Manager. This upgrade replaces the TN795 with the TN2314 processor circuit pack. The hard drive on the new circuit pack contains the new software.

Access keys

The access method for each step is identified by the following keys:

LT	Technician's laptop
LT-IE	Internet Explorer / Web interface on the laptop
SDT	S8100's Windows desktop
SDT-IE	Internet Explorer/Web interface on the S8100's Windows desktop (Note that SDT and SDT-IE are opened inside of LT-IE.)
BS	Bash shell on S8100's Windows desktop
LAC	LAC shell
SAT	System-administration terminal
{...}	Information in braces is for Windows 2000

Upgrade steps

Step		Details	
1	For a direct connection between the technician's laptop and the S8100's service port: **LT** – Change laptop's IP address to 192.11.13.5	**a** **b** **c** **d**	Right-click the 'Network Neighborhood' {My Network Places} icon on the laptop's desktop and select Properties. {Right-click 'PCMIA Ethernet Connection' (or Local Area Connection) and select Properties.} Highlight the TCP/IP icon from the popup window and select Properties. Check the 'Specify an IP address' {'Use the following IP address'} radio button. Enter **192.11.13.5** in the IP address field and **255.255.255.252** in the subnet mask field, and click OK to close the popup windows.
2	**LT-IE** – Disable proxy servers on Internet Explorer.	**a** **b**	Open Internet Explorer and select Tools, Internet Options, the Connections tab, and LAN Settings. Uncheck the 'Use a proxy server' radio button, and click OK to close the popup windows.
3	Connect the laptop to the R9.5 Processor board (TN795).	**a** **b**	Connect a cable from the laptop's PCMCIA Ethernet card to an RJ45 coupler. Connect a cross-over (flip) cable from the coupler to the PCMCIA network-interface card in the TN795's PCMCIA slot.
4	**LT** – Connect to the TN795 processor.	**a** **b**	Click **Start**, **Run**, and enter **telnet 192.11.13.6**. Log in using **lucent3**. – The LAC prompt displays.
5	**LAC** – Open a bash shell by typing **bash** at the LAC prompt.	Type **bash** at the LAC prompt.	
6	**BS** – **Important!** – Display and record the customer's network and product information.	**a** **b**	From the bash shell, execute the following three commands – **setip**, **productid**, **oss**. ***Write down all of this information exactly as it appears on the screen.*** You will need to re-enter this information later.
7	**BS** – Shutdown AUDIX.	Type **shutdown audix**. When the BASH prompt returns (the Audix shutdown takes a few minutes), type **statapp** to verify that AUDIX has shutdown.	
8	**BS** – Exit the bash shell and return to the LAC prompt.	Type **exit**.	
9	**LAC** – Open a SAT window.	Type **definity** to open a SAT window. (The terminal type is 'NTT' {'W2KTT'}.)	
10	**SAT** – Save the DEFINITY translations to the hard drive and logoff the SAT window.	**a** **b**	Execute **save translations**. When the save translations operation is finished, execute **logoff** to logoff the SAT window and return to the LAC prompt.

Step		Details
11	**LT-IE** – Connect to the TN795 processor with Internet Explorer.	Open Internet Explorer on the laptop, type **192.11.13.6** in the URL address bar, and press Enter.
12	**LT-IE** – Backup everything to the PCMCIA card or to a network location. **Note:** If the medium you are backing up to runs out of space, a message will appear noting the files that were not backed up. In this case, find a different backup location or PCMCIA card with enough capacity and rerun the entire backup.	**a** Click 'Administer System' **b** Log in with **lucent3**. **c** Click 'Backup & Restore' under System Maintenance. **d** Click 'Immediate Backup'. **e** Under "Choose Items for Immediate Backup," select everything that is installed. **Note:** If the S8100's internal AUDIX is being used, you must do two backups. First, select the "AUDIX translations, names & messages" radio button in addition to "MultiVantage announcements" and "MultiVantage translations." When the backup finishes, return to the 'Immediate Backup' screen and select only the "AUDIX announcements" radio button and send this backup to the same or a different location. **f** Set Destination to PCMCIA, or click 'Other Location' to send the backup to a network location. **g** Click the Backup button.
13	Verify backup.	Click "Last scheduled backup results", and note the "Time Finished" to verify that the backup finished.
14	**LT-IE** – Record AUDIX extension length. **Note:** You will need to verify the extension length later.	**a** Click the Back icon (on the IE tool bar) twice to return to the Administer System page. **b** From the explorer window, click 'Default AUDIX Settings'. **c** Note whether AUDIX is enabled. If so, click 'AUDIX Extension Length' and record the extension length.
15	**LT-IE** – Shutdown the system.	**a** Click 'Administer System'. **b** Select 'Shutdown or Restart' under the System Maintenance section.
16	The green "Complete" LED on the TN795 faceplate will be flashing during the shutdown process. Wait until this LED is on steady. Then power down the system.	
17	Remove the TN795 Processor board.	
18	Carefully remove the PCMCIA card from the TN795 Processor board and install it in the new TN2314 Processor board.	Do **not** swap the hard drives. A TN795's hard drive will not work on a TN2314.
19	Install the new Processor board into the platform and power up the system.	

Step		Details	
20	Wait approximately 5 minutes, then connect the laptop to the service jack on the front of the TN2314 Processor board.	**a**	Connect a cable from the laptop's PCMCIA Ethernet card to an RJ45 coupler.
		b	Connect a cross-over (flip) cable from the coupler to the RJ45 service jack on the front of the TN2314 Processor board.
21	**LT-IE** – Connect to the TN2314 processor with Internet Explorer.	Open Internet Explorer on the laptop, type **192.11.13.6** in the URL address bar, and press Enter.	
22	**LT-IE** – Open the S8100's desktop. **Note:** Terminal server client and terminal services Active X must be installed on the laptop. The easiest way to do this is to upgrade your Windows 95 laptop's browser to Internet Explorer 5.5.	**a**	Click 'Administer System' and login using **lucent3** for login and password. A domain is not required. Select 'continue' at license agreement window.
		b	Select 'Login to <xxx>' under Remote Control – Terminal Services (where <xxx> is the host name used for this system).
		c	If a VBScript error message appears, click OK.
		d	Click the Connect button (leave the Server field blank).
		e	If a VBScript message appears, click OK (you can resize the Terminal Services screen to full size by pressing ctlr-alt-Pause). A login window will open.
		f	Login using **lucent3**. After login, the S8100's Windows 2000 desktop is displayed.
23	**SDT** – On the S8100's desktop, double-click the time display and set the *time*, *time zone*, *date*, and *Daylight Savings*.	The time display is in the tool tray at the lower right of the desktop.	
24	**SDT** – Disable modem compression.	**a**	Click **Start** → **Settings** → **Control Panel**.
		b	Double-click Phone and Modem Options.
		c	Click the Modems tab.
		d	Select the installed modem and click Properties.
		e	Click the Advanced tab.
		f	Click Change the Default Preferences.
		g	In the Compression drop-down list, select Disabled.
		h	Close each dialog by clicking **OK**, and close the Control Panel window.
25	**SDT** – Open a bash shell window.	Click **Start** → **Run** → **bash**.	
26	**BS** – Verify the software's version.	Type **swversion**. Ensure that the Release number and MultiVantage version number are as expected.	

Step		Details
27	**BS** – Administer the customer's parameters that you wrote down in Step 6, using the setip command.	**setip name=<args>** **setip cust=<args>** **setip dns=<args>** **setip wins=<args>** **setip ras=<args>** Replace each "<args>" with the corresponding parameter you recorded in Step 6.
28	**BS** – Administer the product ID and OSS parameters using the 'productid' and 'oss' commands.	**productid multivantage-product-id <arg>** **productid audix-product-id <arg>** **oss <telno> <retries> <retry_interval>** Replace each "<arg>" with the corresponding parameter you recorded from Step 15. For the **oss** command, enter the **<telno>**, **<retries>**, and **<retry_interval>** parameters separated by spaces; do not enter commas.
29	**BS** – Telnet into the LAC window from the bash.	Execute **telnet 127.1** and login using **lucent3**.
30	**LAC** – Install the new license and password file from the LAC window using the lucent3 login.	For details, see Chapter 3 in *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and the Avaya CMC1 Media Gateways, 555-233-146*.
31	**LAC** – Exit the LAC window and bash shell.	**a** Type **exit**, and close the telnet window. **b** Type **exit** to close the bash window.
32	**SDT** – Open Internet Explorer on the S8100's desktop and login.	**a** Double-click the IE icon on the S8100's desktop. **b** Click 'Administer System'. **c** Log in using **lucent3**. **d** Click Continue on the Notice page.
33	**SDT-IE** – Restore the translations and other backed-up data to the hard drive. **Note:** The Windows logins of **vm**, **sa**, **browse**, and **NTadmin** are reset to their factory defaults. The customer should reset these passwords and reinstall other Windows accounts they may have created.	**a** Click 'Administer System.' **b** Click 'Backup & Restore.' **c** Click 'Restore.' **d** Select the Source for the restore – The Destination or Other location you entered for the backup in Step 12. **e** Click the **Continue** button. Under "These items will be restored from ... ", every item that was backed up to the location specified in Step d will be selected. **f** Click the **Restore** button. **Note:** If you backed up AUDIX announcements in Step 12, you must do two restores. After the first restore, repeat the steps above using the location of the backed up AUDIX announcements for the Source in Step d.
34	**SDT-IE** – When the restore finishes, close Internet Explorer.	
35	**SDT** – Open a bash shell.	Click **Start** → **Run** → **bash**.
36	**BS** – Shutdown every application.	Execute **shutdown all**.

Step		Details
37	**BS** – After the shutdown finishes, restart every application.	Execute **start all**.
38	**BS** – Monitor the startup's progress.	Execute **statapp**.
39	Verify that call processing comes into service.	
40	Verify that voice messaging comes into service.	
41	**BS** – Telnet into the LAC window from the bash.	Execute **telnet 127.1** and logon using **lucent3**.
42	**LAC** – Open a SAT window.	Type **multivantage** to open a SAT window. (The terminal type is W2KTT.)
43	**SAT** – Verify that there is no translation corruption.	If there are corrupted translations, a message will appear when the SAT window opens.
44	**SAT** – Verify that no major or minor alarms are present.	Run **display alarms**.
45	**SAT** – Verify outgoing alarm reports link to INADS.	Run **test inads-link**.
46	**SAT** – Verify no-license/emergency numbers.	Type **change system-parameters features**. See ''Administer No-License/Emergency Numbers'' in *Installation and Upgrades for the Avaya S8100 Media Server with the Avaya G600 and the Avaya CMC1 Media Gateways, 555-233-146.*
47	**SAT** – Save translations.	Run **save trans**.
48	**SAT** – Logoff SAT and exit LAC.	**a** Type **logoff** and respond with **y** to close the SAT session. **b** Type **bash** to go to the bash shell.
49	**BS** – Verify Intuity alarms.	Type **logsend -tTST**.
50	**BS** – Verify GAM alarms.	Type **wrntevent GAM 0 9991**. **Note:** This causes a Major GAM alarm. After the system has called out, enter **cleargamalarm all** at the **BASH prompt** to retire the alarm. This alarm also generates a Maestro case that the INADS group will need to close.
51	**BS** – Close the bash windows.	**a** Type **exit** to close the bash window. **b** Type **exit** to close the LAC window.

Step		Details
52	**LT-IE** – Backup the translations and other data to the PCMCIA card or to a network location.	**a** Click 'Administer System'. **b** Click 'Backup & Restore' under System Maintenance. **c** Click 'Immediate Backup'. **d** Under "Choose Items for Immediate Backup," select everything that is installed. **e** Set Destination to PCMCIA or click 'Other Location' to backup to a network location. **f** Click the Backup button. **Note:** If the medium you are backing up to runs out of space, a message will appear noting the files that didn't get backed up.
53	Close Internet Explorer on the S8100's desktop and on the laptop.	
	SECURITY ALERT: When you are finished with the upgrade procedures, you should restore your laptop to its original configuration.	

Contents

Checklists and job aids 5

- Initial installation 5
- System initialization 8
- Administer INTUITY AUDIX digital networking 11
- Upgrade an S8100's R10+ software using a CD 12
  - Access keys 12
  - Upgrade steps 13
- Replace an S8100's hard drive 20
  - Access keys 20
  - Upgrade steps 20
- Upgrade an S8100's R9.5 software by replacing the S8100 26
  - Access keys 26
  - Upgrade steps 27

About this book 47

- Overview 47
- Audience 47
- Using this book 48
- Conventions 50
  - Physical dimensions 50
  - Terminology 50
  - Typography 50
  - Commands 50
    - User input 51
    - System output and field names 51
- Related documents 51
- Technical assistance 52
  - Within the US 52
  - Outside the US 52
- Trademarks 52
- Security-alert and safety labels 52

- Safety precautions 53
  - Electromagnetic interference 53
  - Customer's safety responsibilities 53
  - Antistatic protection 53
  - Control circuit packs versus power 54
- Avaya Product Documentation web page 54
- Avaya Publications Center 54
- Sending comments 55

1 Install and cable a G600 cabinet 57

- Section I – S8100 with a G600 installation 58
- Site requirements 58
- Check customer's order 59
- Correct shipping errors 59
- Unpack and inspect 60
- Install and cable a G600 cabinet 65
  - Verify the carrier address ID on G600 cabinets 65
  - Floor mount a G600 cabinet 67
  - Rack mount a G600 cabinet 68
  - Rack mount two G600 cabinets 71
- Check AC power and ground for G600 72
  - Check AC power 72
  - Approved grounds 73
    - Approved floor grounds 73
  - Uninterruptible power supply 74
  - Cabinet's power switch 74
  - Connect cabinet's grounds and other grounds 75
  - Install coupled bonding conductor 78
  - Connect the power cords 78
- Cable a G600 system 78
  - Install Processor Interface cable 79
  - Cable a 2-cabinet G600 system 80
  - Cable a 3-cabinet G600 system 84
- Install G600 patch panels and external modem 84
  - Install patch panels and shelf 84
  - Install the external modem 85

- Install equipment-room hardware for G600 86
  - Cross-connect the cabinet to the patch panels 86
  - Allowed circuit packs 86
  - Disallowed circuit packs 89
  - Circuit-pack installation 91
    - Circuit-pack slot loading 91
  - Off-premises circuit protection 93
  - Install sneak fuse panels 94
- Set ringing option for G600 97
- Section II – Install telephones and make auxiliary connections 99
- Install and wire telephones and other equipment 99
    - Telephone connection examples 99
    - Connect adjunct power 100
    - Station wiring examples 101
    - Analog tie trunk example 103
    - Digital tie trunk example 103
    - Cable examples for tie trunk connectivity 104
    - DS1 tie trunks between collocated systems 105
    - 3- and 4-pair modularity 105
    - Adjunct power connections 106
    - Auxiliary power 108
  - Install attendant console – optional 108
    - Hard-wire bridging 108
    - Dual wiring of 2-wire and 4-wire endpoints 108
  - Install 26B1 selector console – optional 109
  - 1152A1 Mid-Span power-distribution unit 109
    - Important safety instructions 109
    - Using the 1152A1 PDU 110
    - Connect the 1152A1 PDU 110
    - Connect the cables 111
- Connect external alarms and auxiliary connections 113
    - Alarm input 113
    - Alarm output 113
    - UPS alarm connection 114
    - Emergency transfer and auxiliary power 115
  - Telephone pin designations 115

- Install the BRI terminating resistor 116
  - Terminating-resistor adapter 116
  - Closet-mounted (110RA1-12) 117
- Install multipoint adapters 119
  - BR851-B adapter (T-adapter) 119
  - 367A adapter 120
  - Basic multipoint installation distances 121
- Install off-premises station wiring 122
  - Install off-premises or out-of-building stations 122
    - Analog off-premises stations 122
    - Circuit protectors 124
    - Digital out-of-building telephones 125
- Install emergency-transfer panel and associated telephones 127
  - Install the emergency-transfer panel 127
    - Install telephone for power-transfer unit 133
- Connect modem to telephone network 134
- Connect modem 135
  - Option settings for external modem 135
- Set neon voltage to prevent ring ping 136
- Complete installation 137
- View LEDs to determine power and fan alarm state 138

2 Connectivity and access to an S8100 system 139

- Physical connections 139
  - Direct connection to the RJ45 service jack 140
    - Connect the laptop to S8100 system 140
    - Configure the laptop (laptop running WINDOWS 95) 142
    - Connect S8100 system to laptop's CD-ROM drive (laptop running WINDOWS 95) 144
    - Restore the laptop's settings (laptop running WINDOWS 95) 145
    - Configure the laptop (laptop running WINDOWS 2000) 146
    - Connect S8100 system to laptop's CD-ROM drive (laptop running WINDOWS 2000) 146
    - Restore the laptop's settings (laptop running WINDOWS 2000) 148
  - Direct connection with a local monitor/ mouse/keyboard 149
  - Connection via customer's LAN 149

Connection via RAS (modem) dial up 149
Create a connection icon 150
- Access methods 151
Via a Telnet session 152
Via a web browser session 153
Logging into the S8100 Windows 2000 desktop 156
Remotely using Avaya Site Administration 156
Dial-in permissions to an existing login 156
Creating a login for remote access 156
Starting an Avaya Site Administration session 157
- Logins for the S8100 158
Avaya personnel logins 158
Avaya business partner and dealer logins 158

3 System initialization 159

- Connectivity and access to the S8100 system 160
- Configure DHCP and TFTP servers 161
DHCP server 161
TFTP server 162
- Preliminary tasks 162
Power up and observe LEDs 162
Connect the laptop computer to S8100 162
Start a Telnet session 162
Verify the software's version number 163
Determine the serial number 163
Set up customer's LAN parameters 163
- License file, password file, and installation script overview 164
Using the Feature Extraction tool (for upgrades from pre-R10 only) 165
- Obtain the license and password files 165
RFA information requirements for new installations 165
Go to the RFA web site 166
- Obtain the installation script file 166
Direct channels 166
Indirect channels 167

- Install the password file, license file, and installation scripts 168
  - Copy files to the server 168
  - Install the password, license, and installation-script file 169
  - License file installation failure 169
- Manually set S8100's customer-related information (alternative to ART) 170
  - Manually setting RAS IP address: 170
  - Manually setting product ID: 171
  - Manually setting alarm origination and alarm-destination number 171
- Administer no-license/emergency numbers 171
  - Alerts/notifications 172
- Test alarm call out 172
  - Communication Manager alarm test 173
  - INTUITY alarm test 173
  - Windows 2000 server alarm test 173
  - Resolve alarms 173
- Check system's status 173
- Enable customer logins 173
  - Enable INTUITY AUDIX logins 174
  - Enable customer's web logins 174
  - Enable S8100 Logins 174
- Administer S8100 174
  - S8100 commands 174
  - Set system date and time 174
    - Using Windows 2000 174
    - Using systime 175
    - Using a local command-line interface (CLI) 175
- Remote dial-in 175
- Set up country-specific call-progress tones 176
- Enable and disable SNMP 178
- Check customer option screen 178
- Set country options 179
- Check system's status 180

- Set up your system 180
  - Set country options 180
  - Administer the attendant console 181
  - Add translations 181
  - Administer telephone features 182
  - Place a test call 182
  - Test INADS callout 182
- Setup call-detail recording(CDR) 182
  - Share CDR data 183
  - Map a shared CDR directory 183
  - Set call-collection interface 184
  - Verify call-record collection 184
- Call accounting 185
- Administer Communication Manager for INTUITY AUDIX initialization 185
  - Check the dial plan 185
  - Check hunt groups 186
  - Check class of service 187
  - Check class of restriction 187
  - Change the dial plan 188
  - Add AUDIX ports 189
  - Make a hunt group 191
  - Change coverage path 193
  - Add test phones 193
  - Save translations 194
- INTUITY AUDIX administration 194
  - INTUITY AUDIX commands 194
    - Adding an INTUITY AUDIX subscriber 194
- Download Avaya Site Administration 197
  - Start an Avaya Site Administration session 199
- Administer SNMP 199
  - Configure SNMP trap destinations 200
  - Configure SNMP community strings 202
  - Start and stop SNMP 203
- Schedule backups 205
  - Add a scheduled backup 205

4 INTUITY AUDIX digital networking 207

- Initial administration tasks 207
- View the Feature Options window 209
- Change number of administered remote users 210
- Administer networking channels 211
- Change local machine's information 212
  - Change a local machine's profile 212
  - Complete the Local Machine Administration window 216
  - Add a remote machine 216
  - Complete the Digital Machine Administration window (via web browser) 217
  - Complete the Machine Profile screen for the remote machine (via AUDIX) 219
  - Perform a full remote update 223
  - Reset automatic deletion of nonadministered remote users 223
  - View remote extensions 224

5 Upgrade and repair procedures 225

- Replace a TN795 Processor circuit pack 225
  - Inventory existing features on the pre-R10 switch and obtain a license file 225
  - Replacing a TN795 with a TN2314 226
- Replace the TN2314 Processor circuit pack 226
- Replace the hard disk 226
- Download firmware to port circuit packs 227

6 Hardware additions 229

- Add circuit packs 229
- Add IP trunk 230
- Add remote office 230
- Add C-LAN functionality 230
  - Add a TN799DP C-LAN circuit pack 230
    - Install the TN799DP 231
    - Administer the TN799DP on the SAT 231
    - Test the external connection to the LAN 232
  - Communication Manger 233
- Add TN464GP/TN2464BP with echo cancellation 234

- Add CO, FX, WATS, and PCOL 236
  - Requirements 236
  - Installation 236
- Add DID trunks 236
  - Requirements 236
  - Installation 237
- Add Tie trunks 237
  - Requirements 237
  - Installation 237
- Add DS1 tie and OPS 238
  - Service interruption 238
- Add speech synthesis 239
- Add Code Calling access 239
- Multiple integrated recorded announcements 239
  - TN750C Announcement circuit pack 240
    - Add TN750C circuit pack 240
    - Move a single announcement to another Announcement circuit pack 240
  - CWY1 announcements 240
    - Installing CWY1 announcements 241
- Add ISDN-PRI 242
  - T1 (North American standard) 242
  - E1 (international standard) 242
  - Add circuit packs 243
  - Install cables 243
  - Enter added translations 243
  - Resolve alarms 243
  - Save translations 243
- DEFINITY LAN gateway (DLG) 243
  - Corresident DLG 244

7 Avaya Site Administration 245

- Avaya Site Administration overview 245
- Interactions with switches and voice-mail systems 248
- Components of Avaya Site Administration 249
- How Avaya Site Administration works 251
- Avaya Site Administration help 251

- Install Avaya Site Administration 252
- Configure Avaya Site Administration 253
  - Add an S8100 switch-administration item 253
  - Add S8100 voice-mail administration item 254
  - Start a switch-administration session 254
    - To launch a GEDI session: 254
    - To launch an emulation session: 255
  - Start a voice-mail administration session 256

8 Message Manager 257

- Download Message Manager 257
- Install Message Manager 257

9 Troubleshooting 259

- Install wizard's error messages 259
- Platform's troubleshooting commands 261
- Modem's configuration and administration 262
  - Verify INADS modem settings 262
    - No external modem installed 262
    - External modem installed 262
  - Verify external modem option settings 262
  - External modem not used 263
  - Configure the installed modem 264
  - Test the external modem 264

10 Security and copy protection 265

- Software copy-protection mechanisms 265
  - Feature protection 265
  - Copy protection 265

A Cable pinouts 267

- Set TN760E Tie Trunk's options 267
- Set TN464GP T1/E1's options 269
- Connector and cable diagrams – pinout charts 270
  - Pinout for Processor's external cable 272

B Set up customer logins 285

- Customer access 285
- Windows logins for customers 286
  - Windows login types for customers 286
    - Administrator login 286
    - INTUITY AUDIX logins 287
    - Customer's web-access logins 288
  - Enabling Windows 2000 customer logins 290
    - Set up login accounts 290
- Communication Manager logins for customers 291
  - Forced password aging 292
  - Logoff notification 292
  - Super user 292
  - Administer login command permissions 292
  - Communication Manager commands for user login 293
    - Password expiration 294

C Miscellaneous procedures 295

- Setting the name of the switch 295
  - Setting the Windows name 295
  - Updating INTUITY AUDIX machine name 296
  - Restarting INTUITY AUDIX 296
  - Changing system name 296
- Connect to SAT session via Telnet 296
  - Function-key sequences for W2KTT terminal type 298
- Installing INTUITY languages other than English 299
  - Laptop configuration for Windows 95/98/NT 299
  - Installing INTUITY languages 301
- Perform backup 302
  - Backup using a LAN-resident PC 303
  - Backup using an S8100 desktop 304
  - Enter backup commands 304
- Backup via the web interface 305
  - Perform immediate backup 308
  - View backup progress 309
  - Back up to a LAN address 309

View scheduled backups 311
Access backup information 311
Perform restore 313
- Enable/disable embedded messaging 314
Impact on maintenance 314
- Access Diskeeper software to defragment the disk 315
Change the default times on Diskeeper 315

D Recovery 317

- S8100 system-level shutdown and restart 317
- Communication Manager software reset (recovery) 319
Reset System 1 (Communication Manager warm start) 320
Reset System 2 (Communication Manager cold start) 320
Reset System 3 (Communication Manager reboot) 320
Reset System 4 (Communication Manager reboot) 320
Reset System 5 (system reboot) 320

E LED boot sequence/ TN2314 Processor 321

- LED boot sequence 321
TN2314 Processor circuit pack 321
TN2314 Processor circuit pack's LEDs (after booting) 322
LED states 324

F Status LEDs 325

- Attendant console's LEDs 325
- Other circuit packs 325
Circuit packs' status LEDs 325
Power supply's LEDs 327

G GAS commands in bash 329

- Avaya (Lucent) access controller bash commands 329
- LAC commands 331
- setip command 332
Display current settings 332
Set the machine name in Windows 332
Set RAS IP address 333

Set the customer's LAN, DNS, and WINS information 333
Set LAN address 333
Set DNS addresses and host name 333
Set WINS addresses 334
- Other commands 334
ftpserv command 334
statapp command 334
net user commands 335

H Installation connectivity quick reference 337

I Map CD-ROM for an S8100 upgrade 339

- Prepare to access the S8100 339
Activate the Guest account 339
Check the Guest account's current setting 339
Enable the Guest account 340
Verify the Guest account's new setting 340
Share the laptop's CD-ROM drive 340
- Connect to and access the S8100 341
Prepare to access the S8100's desktop 341
Connect to the S8100 341
- Map to the laptop's CD-ROM drive 342

J Install and cable a CMC1 cabinet 343

- Check customer's order 343
- Correct shipping errors 344
- Unpack and inspect 344
- Install an S8100 with a CMC1 system cabinet 348
Verify the carrier address ID on CMC1 cabinets 348
Floor mount the CMC1 cabinet 350
Wall mount the CMC1 cabinets 350
Install plywood backing on wall 351
Install wall-mounted cabinet 352
Install three vertically mounted cabinets 354
Install two cabinets vertically and one horizontally 355
Install left and right panels – wall mount 356

- Check AC power and ground for CMC1 357
  - Check AC power 357
  - Approved grounds 358
    - Approved floor grounds 358
  - Uninterruptible power supply 359
  - Cabinet's power switch 359
  - Connect cabinet's grounds and other grounds 360
    - Install the ground block and ground wire on cabinets 360
  - Install coupled bonding conductor 364
  - Connect and route the power cords 364
- Cable a CMC1 system 367
  - Install Processor Interface cable and TDM-/LAN-bus terminators 367
  - Cable 3-cabinet CMC1 system 368
    - Vertically mounted system 368
    - Vertically and horizontally mounted system 369
- Install CMC1 main distribution frame (MDF) and external modem 370
  - Install the MDF on CMC1 370
    - Bottom-mounted MDF with modem 370
  - Install the external modem 371
- Install equipment-room hardware for CMC1 372
  - Cross-connect the cabinet to the MDF 372
  - Allowed circuit packs 372
  - Disallowed circuit packs 375
  - Circuit pack installation 377
    - Circuit-pack slot loading 377
  - Off-premises circuit protection 380
  - Install sneak fuse panels 381
  - Label the main distribution frame 383
- Set ringing option for CMC1 385

K Identify a hard disk for PCN1413b 387

Glossary 391

Index 401

About this book

Overview

This document provides procedures to install, upgrade, or add to an Avaya S8100 Media Server with an Avaya G600 Media Gateway (formerly called IP600). This document also provides procedures to replace, upgrade, or add to an Avaya S8100 Media Server with an Avaya CMC1 Media Gateway (formerly called DEFINITY ONE). Within both physical platforms, the S8100 media server resides on a TN2314 circuit pack.

The current offer, S8100 with G600, is a high-functionality system for customers needing from 20 to 450 stations – which can be any combination of IP, DCP, ISDN, and analog stations – and up to 300 trunks. A G600 fits well in a communications environment with converged IP data and voice-over-IP (VoIP) data. This offer provides Avaya Communication Manager and INTUITY™ AUDIX® messaging on a single hardware platform.

The legacy offer, S8100 with CMC1, is a high-functionality communications system for customers with similar line requirements and growth potential, 20 – 40 stations, with growth potential to 240 stations and up to 300 trunks. This legacy offer also provides Communication Manager and INTUITY AUDIX messaging on a single hardware platform.

Audience

The primary audience for this book is trained field installation and maintenance personnel performing initial installations, migrations, and upgrades of the S8100 media server with the G600 or CMC1 media gateways. Installation technicians are assumed to have training in Windows 2000 and local area networks (LANs). Secondary audiences include the Technical Service Center (TSC) personnel.

Using this book

This book provides step-by-step procedures for installing or upgrading S8100 systems that implement the Communication Manager features..

Checklists	The initial checklists summarize the steps for several common installation procedures – installing and initializing an S8100 system and for administering INTUITY AUDIX digital networking. Each step provides a link to more detailed information later in the book.
Job Aids	The following Job Aids summarize the steps for several common upgrade procedures – for pre-R10 systems (replacing the processor board), for R10 or later (replacing the hard drive), and for R10 or later (new software on a CD-ROM). An experienced technician can use a Job Aid as stand-alone documentation.
Chapter 1	Use this chapter to initially install and cable an S8100 with G600.
Chapter 2	This chapter describes the procedures for connecting to and accessing an S8100 server.
Chapter 3	This chapter describes the procedures for initializing the S8100 system, including the installation of the license file, password file, and installation script file, and other system services.
Chapter 4	Use this chapter to administer INTUITY AUDIX digital networking.
Chapter 5	Use this chapter along with the job aids to upgrade or repair an S8100 system.
Chapter 6	Use this chapter to add or upgrade a circuit pack's hardware and software or to administer the features provided by a new circuit pack.
Chapter 7	Use this chapter to set up Avaya Site Administration.
Chapter 8	Use this chapter to install Message Manager.
Chapter 9	This chapter provides some troubleshooting information for problems that may occur during installation of an S8100 server or an external modem.
Chapter 10	This chapter briefly describes the copy-protection aspects of an S8100 media server's software.
Appendix A	This appendix lists pinout information for the essential circuit packs and cables.
Appendix B	Refer to this appendix when setting up a customer's logins or when installing Avaya Site Manager or Message Manager.
Appendix C	This appendix contains procedures for several installation and maintenance tasks not covered elsewhere in the book.
Appendix D	Use this appendix when performing shutdown and reset/reboot procedures.
Appendix E	This appendix describes the TN2314 processor's LED boot sequence and LED states.
Appendix F	This appendix provides information about an S8100 system's status LEDs.
Appendix G	This appendix summarizes the Bash and LAC commands.

Appendix H	This appendix briefly summarizes the various connections and access methods to an S8100 system.
Appendix I	Use this appendix to map a laptop's CD-ROM drive for an S8100 upgrade.
Appendix J	Use this appendix to initially install and cable an S8100 with CMC1.
Appendix K	Use this appendix to identify the correct hard disks to be replaced under PCN1413b.

Conventions

This section describes the conventions used in this book.

Physical dimensions

- Each physical dimension is in English units, followed by parentheses with the equivalent metric dimension.
- Each wire gauge is in AWG (American wire guage), followed by parentheses with the area of the wire's metallic cross-section in square millimeters.

Terminology

- Communication Manager replaces *MultiVantage software* to refer to the application that provides call control and telephony features.
- *System* is a general term that encompasses every reference to the Avaya Media Server or Gateway with Communication Manager.
- *S8100 system* is used as an abbreviation for either the Avaya S8100 Media Server with the Avaya G600 Media Gateway or the Avaya S8100 Media Server with the Avaya CMC1 Media Gateway.
- Avaya S8100 Media Server is abbreviated as *S8100 server.*
- CMC1 Media Gateway is abbreviated as *CMC1*.
- G600 Media Gateway is abbreviated as *G600.*
- Refer to *Technical Monthly: Reference Guide for Circuit Pack Vintages and Change Notices* for current information about usable vintages of a specific circuit pack's code (including its suffix).

Typography

This section describes the typographical conventions for commands, keys, user input, system output, and field names.

Commands

- Commands are in **bold** type. Example:

  Type **change-switch-time-zone**, and press **Enter**.

- Command variables are in ***bold italic*** type when they are part of what you must type, and in *plain italic* type when they are not part of what you must type. Example:

  Type **ch *machine_name***, where *machine_name* is the name of the call delivery machine.

- Command options are in **bold** type inside square brackets. Example:

  At the DOS prompt, type **copybcf [-F34]**.

User input

- User input is in **bold** type, whether you must type the input, select the input from a menu, or click a button or similar element on a screen or a web page. Examples:
  - Type **exit**, and then press **Enter**.
  - On the **File** menu, click **Save**.
  - On the Network Gateway page, click **Configure** → **Hardware**.

System output and field names

System output and field names on the screen are in `monospaced` type.

Related documents

The following documents provide supplemental information when installing an S8100 with G600 or CMC1 system:

- Hardware Guide for Avaya Communication Manager
- *DEFINITY® Communications System Generic 1 and Generic 3 Main Distribution Field Design* (555-230-630)
- *DEFINITY® Enterprise Communications Server and System 75 and System 85 Terminals and Adjuncts Reference* (555-015-201)
- *Installation, Upgrades, and Additions for Avaya CMC1 Media Gateways* (555-233-118)
- *Installation for Adjuncts and Peripherals for* Avaya Communication Manager (555-233-116)
- *Administrator's Guide for Avaya Communication Manager* (555-233-506)
- *Administration for Network Connectivity for Avaya Communication Manager* (555-233-504)
- *Maintenance for DEFINITY Server CSI* (555-233-119)
- *DEFINITY ONE Communications System AUDIX Administration Command Line Quick Reference Card* (555-233-737)
- *Maintenance for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways* (555-233-149)
- *Overview for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways* (555-233-231)
- *Avaya Communication Manager Little Instruction Book for Basic Administration* (555-233-756)
- *Avaya Communication Manager Little Instruction Book for Advanced Administration* (555-233-757)
- *Avaya Communication Manager Little Instruction Book for Basic Diagnostics* (555-233-758)
- *Getting Started with the Avaya R300 Remote Office* (555-233-769)
- *MAX 3000 Installation and Basic Configuration Guide* (555-233-768)
- *Avaya Communication Manager Toll Fraud and Security Handbook* (555-025-600)

Technical assistance

Avaya provides the following resources for technical assistance.

Within the US

For help with:

- Feature administration and system applications, call the Avaya DEFINITY Helpline: **1-800-225-7585**
- Maintenance and repair, call the Avaya National Customer Care Support Line: **1-800-242-2121**
- Toll fraud, call Avaya Toll Fraud Intervention: **1-800-643-2353**

  Avaya offers services that can reduce toll-fraud liabilities. For more information, contact your Avaya representative.
- Other security issues, call Avaya Corporate Security: **1-800-822-9009**

Outside the US

For any non-US location, contact your local Avaya-authorized dealer for additional help.

Trademarks

Every trademark identified by the ® or ™ is a registered trademark or trademark, respectively, of Avaya Inc. Every other trademark is the property of its respective owner.

Security-alert and safety labels

Observe every caution, warning, and danger statement to help prevent loss of service, equipment damage, personal injury, and security problems. This book uses the following security-alert and safety labels:

SECURITY ALERT:
A security alert calls attention to a situation that can increase the potential for unauthorized use of a telecommunications system.

CAUTION:
A caution statement calls attention to a situation that can result in harm to software, loss of data, or an interruption in service.

WARNING:
A warning statement calls attention to a situation that can result in harm to hardware or equipment.

WARNING:
An ESD warning calls attention to a situation that can result in ESD damage to electronic components.

DANGER:
A danger statement calls attention to a situation that can result in harm to personnel.

Safety precautions

When performing maintenance or translation procedures on the system, users must observe certain precautions. Observe every caution, warning, and danger admonishment to prevent loss of service, possible equipment damage, and possible personal injury. In addition, the following precautions regarding electromagnetic interference (EMI) and static electricity must be observed:

Electromagnetic interference

This equipment generates, uses, and can radiate radio frequency (RF) energy. Electromagnetic fields radiating from the switch may cause noise in the customer's equipment. If the equipment is not installed and used in accordance with the instruction book, radio interference may result.

WARNING:
To maintain the EMI integrity of the system, maintenance personnel ***must ensure*** that every cabinet panel, cover, and so forth, is firmly secured before leaving the customer's premises.

Customer's safety responsibilities

The customer has the responsibility to provide – a properly installed standard 19″rack, adequate AC power, approved grounding, and sufficient ventilation.

For more information, see Site requirements on page 58.

Antistatic protection

WARNING:
When handling circuit packs or any components of an S8100, always wear an antistatic wrist ground strap. Connect the strap to the ESD ground jack or an approved ground such as an unpainted metal surface on the S8100.

Control circuit packs versus power

WARNING:
When the system's power is on, the S8100 server (TN2314) can be removed ***only*** after the TN2314's shutdown procedure has completed.

WARNING:
The control circuit packs with white labels ***cannot*** be removed or installed when the system's power is on. The port circuit packs with gray labels (older versions had purple labels) ***can*** be removed or installed when the power is on.

Avaya Product Documentation web page

You can download the latest version of this book, *Replace variable w/ DocNumber*, from the Avaya web site. You must have access to the Internet, and a copy of Acrobat Reader must be installed on your personal computer.

Avaya makes every effort to ensure that the information in this book is complete and accurate. However, information can change after we publish this book. The Avaya web site may contain new product information and updates to the information in this book.

To download the latest version of this book:

1. Access the Avaya web site at http://support.avaya.com.
2. Click **Product Documentation**. The system displays the Welcome to Product Documentation page.
3. Type **Replace variable w/ DocNumber** in the search window and then click **Search**. The system displays the Product Documentation Search Results page.
4. Scroll down to find the latest issue number, and then click the book title that is to the right of the latest issue number.
5. On the next page, scroll down and click one of the following options:
   - **PDF Format** to download the book in regular PDF format
   - **ZIP Format** to download the book in zipped PDF format

Avaya Publications Center

In addition to this book, other description, installation, maintenance, and administration books, and documentation library CDs, are available.

This document (555-233-146) and any other Avaya documentation can be ordered directly from the Avaya Publications Center toll free at 1-800-457-1235 (voice) and 1-800-457-1764 (fax). International customers should use +1.207.866.6701 (voice) and +1.207.626.7269 (fax).

Sending comments

Avaya welcomes your comments about this book. To reach us by:

- Mail, send your comments to:

  Avaya Inc.
  Product Documentation Group
  Room B3-H13
  1300 W. 120 Ave.
  Westminster, CO 80234 USA

- E-mail, send your comments to:
  document@avaya.com

- Fax, send your comments to:
  1-303-538-1741

Please be sure to include the name and number (Replace variable w/ DocNumber) of this book.

1 Install and cable a G600 cabinet

This chapter describes procedures for installing and cabling the cabinet to physically connect and access an S8100 Media Server with G600 Media Gateways. Also, for either a G600 or CMC1 Media Gateway, Section II of this chapter describes procedures for installing telephones and making auxiliary connections.

NOTE:
A G600 is a rack-mounted cabinet, whereas a CMC1 is a wall- or table-mounted cabinet. For information about installing a CMC1 cabinet, see Appendix I – Install and cable a CMC1 cabinet on page 343.

NOTE:
The physical installation of a G600 cabinet is similar to a ProLogix cabinet. The cabling is also similar, except for the Processor Interface cable (multileg cable). Do not access applications, such as Communication Manager, until installation and cabling of the cabinet are finished. Your configuration can consist of an S8100 Media Server with 1, 2, or 3 G600 Media Gateways.

This chapter is organized as follows:

Section I – S8100 with a G600 installation on page 58

- Site requirements on page 58
- Check customer's order on page 59
- Correct shipping errors on page 59
- Unpack and inspect on page 60
- Install and cable a G600 cabinet on page 65
- Check AC power and ground for G600 on page 72
- Cable a G600 system on page 78
- Install G600 patch panels and external modem on page 84
- Install equipment-room hardware for G600 on page 86
- Set ringing option for G600 on page 97

Section II – Install telephones and make auxiliary connections on page 99

- Install and wire telephones and other equipment on page 99
- Connect external alarms and auxiliary connections on page 113
- Install the BRI terminating resistor on page 116
- Install multipoint adapters on page 119
- Install off-premises station wiring on page 122
- Install emergency-transfer panel and associated telephones on page 127
- Connect modem on page 135
- Connect modem to telephone network on page 134
- Set neon voltage to prevent ring ping on page 136
- Complete installation on page 137
- View LEDs to determine power and fan alarm state on page 138

Section I – S8100 with a G600 installation

This section covers procedures for installing the S8100 server with the G600 Media Gateway.

Site requirements

A G600 mounts in a standard 19-inch (48-cm) data rack that has been properly preinstalled and secured per local code and the EIA 310 (or equivalent) standards. The customer is responsible for providing the rack and having it installed and secured prior to G600 installation. This also applies to providing AC power to the rack and approved grounding. Technicians who are trained to install G600s do not typically have the tools or proper training to install data racks.

If floor-mounted (single cabinet only), the technician is responsible for installing the cabinet per local code.

The G600 cabinet's dimensions are 12 inches (7µ) high × 22 inches deep × 19 inches wide. The G600 cabinet can be mounted at its midpoint by removing the mounting brackets and remounting them at a medial position.

Installation requires 1 foot (30 cm) of clearance in the rear, and 18 inches (45 cm) of clearance in the front, which is consistent with the EIA 310 data rack standards. In a 2- or 3-cabinet configuration, the dimensions of the TDM/LAN cable require that one cabinet be mounted directly over the other (flush).

The G600 should be installed in a well-ventilated area. Maximum equipment performance is achieved at an ambient temperature between 40 and 120° F (4 and 49° C) for short-term operation (no more than 72 consecutive hours or 15 days in a year) and up to 110° F (43° C) for continuous operation. The relative humidity range is 10 to 95% at up to 84° F (29° C). Above this, maximum relative humidity decreases from 95% down to 32% at 120° F (49° C). Installations outside these limits may reduce system life or affect operation. The recommended temperature and humidity range is 65 to 85° F (18 to 29° C) at 20 to 60% relative humidity.

The other Environmental Considerations and System Protection requirements described in the *Hardware Guide for Avaya Communication Manager* under "Site Requirements" apply to the G600 as well.

Table 1: Power sources and receptacles for AC-powered cabinets

Cabinet's style and power-distribution unit	Power sources	Power input receptacles
Rack-mounted cabinet – AC power supply (650A integrated power supply) No integrated DC power supply – DC rectifiers can be used if desired; follow manufacturer's instructions.	Single-phase 120-VAC source, with neutral Single-phase 240-VAC source, with neutral	120-VAC, 60-Hz NEMA 5-15R receptacle 240-VAC, 50-Hz IEC 320 receptacle Installations in Japan use country-specific 100-/200-VAC, 50-/60-Hz receptacles

Table 2: Circuit breakers for AC-powered cabinets

Cabinet's type	Circuit breaker's size
Rack-mounted cabinet (120 VAC, 60 Hz)	15 A
Rack-mounted cabinet (240 VAC, 50 Hz)	10 A

Check customer's order

1. Check the customer's order and the shipping packing lists to confirm that all equipment is included.
2. Report missing equipment to an Avaya representative.
3. Check the system's adjuncts, and report any damage according to local shipping instructions.

Correct shipping errors

1. Red-tag any defective or over-shipped equipment, and return it according to instuctions from National Parts.
2. Direct any short-shipped reports to National Parts. Contact the appropriate location for specific instructions. For a streamlined implementation, call 1-800-772-5409.

Unpack and inspect

DANGER:
Use lifting precautions. An empty G600 weighs 35 – 39 lbs (15.8 – 17.6 kg).

1 Verify the equipment received. See Figure 1, Equipment packed with a single G600 cabinet, on page 61. Actual equipment may vary in appearance and may ship in separate packages. Equipment comcodes are listed in Table 3, Comcodes for equipment used with G600, on page 63.

2 Before mounting the G600, remove the door by opening and then lifting it straight up and off the hinge pins.

NOTE:
The G600's power cord, software and documentation CDs, Processor Interface cable, wrist strap, and cabinet's feet are shipped inside the cabinet's accessory compartment. See Figure 1, Equipment packed with a single G600 cabinet, on page 61. The optional G600 port cabinet is shipped with AC power cord or international power-cord kit, mounting kit, TDM-/LAN-bus cable, and EMI gasket.

Figure 1: Equipment packed with a single G600 cabinet

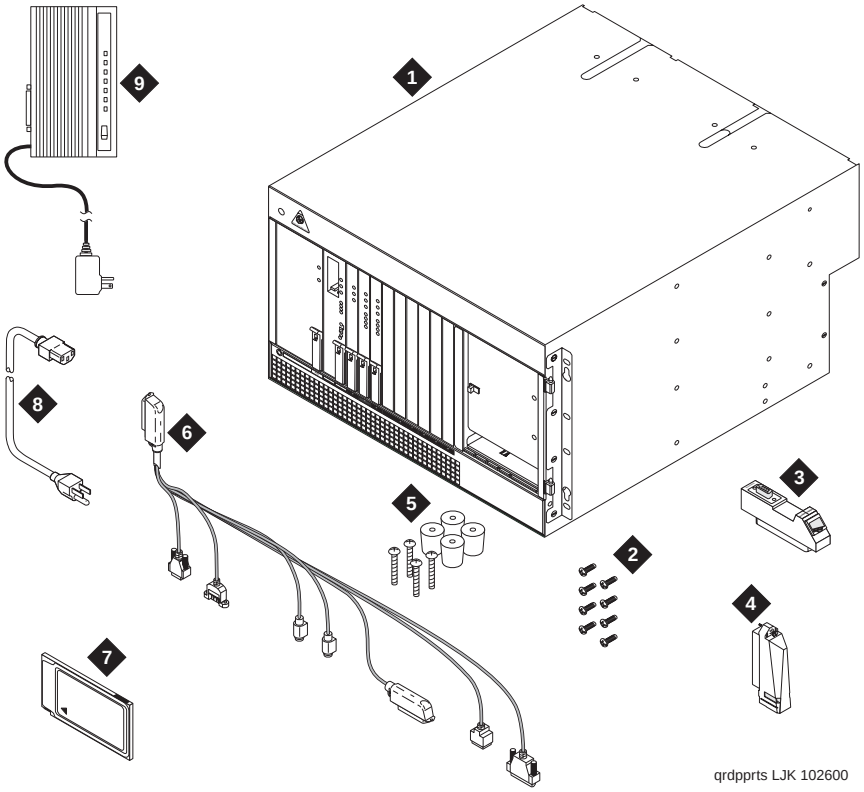


Figure notes

1 G600 cabinet with 650A power supply

2 Screws (for rack mounting)

3 IP Media Processor adapter (may be preinstalled)

4 259A adapter for C-LAN

5 Cabinet's feet and screws

6 Processor Interface cable

7 Flash card (backup)

8 AC power cord (NEMA 5-15P or IEC 320) or international power-cord kit

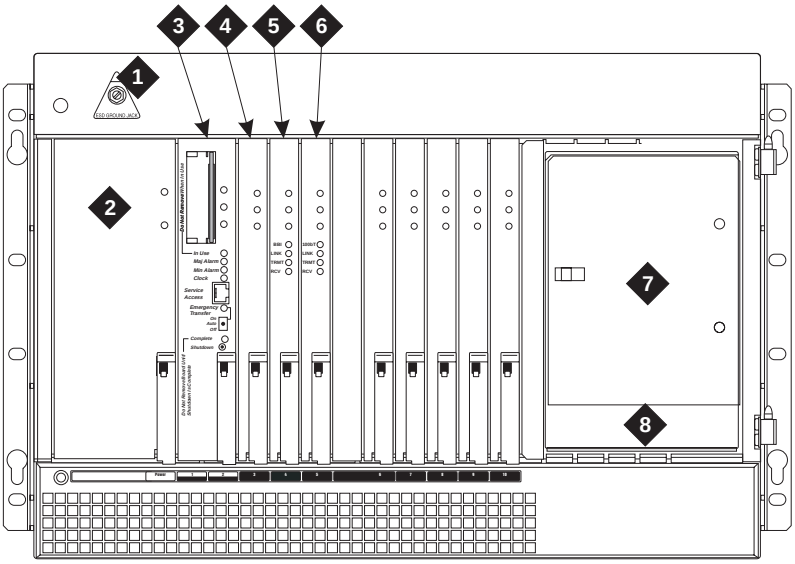
9 External modem (purchased separately)

The following circuit packs are shipped with the G600:

- TN2314 Processor
- TN744E Call Classifier/Detector
- TN2302 Media Processor
- TN799DP C-LAN

The remote modem's shelf is also included with the packaging.

Figure 2: Front view of a G600



scdpff02 KLC 071902

Figure notes

1	ESD ground jack	**5**	TN2302 Media Processor
2	650A power supply	**6**	TN799DP C-LAN
3	TN2314 Processor circuit pack	**7**	Accessory compartment
4	TN744E Call Classifier/Detector	**8**	Fiber-optic pass through

Table 3, Comcodes for equipment used with G600, on page 63 lists the comcodes for equipment used with the G600. If an item is marked with an "×" in the "Optional" column and depending on the site's configuration, the item may be unnecessary.

Table 3: Comcodes for equipment used with G600 ***1 of 2***

Comcode	Description	Optional
848627204	Door	
848627147	Bottom panel	
700017932	Mounting kit (screws)	
700019292	Time-division multiplexing/local area network (TDM/LAN) bus cable (for connection between the control cabinet and a port cabinet)	×
848525887	IP Media Processor adapter	
102631413	259A adapter for C-LAN	
700017916	Rack-mounting guide	
700018021	EMI gasket	×
700017924	EMI gasket's installation instructions	×
848627188	Fan assembly	
700012925	Remote modem's shelf	×
700012909	24-port patch panel	×
700012917	8-port patch panel	×
601929763	Processor Interface cable (multileg cable), TN2314	
601929763	TN2314 Processor circuit pack	
848320800	Hard disk programmed	
700169121	External modem	×
601929920	Software CDs	
408166783	PCMCIA flash card (for backup)	
105631527	Time-division multiplexing/local area network bus (TDM-/LAN-bus) terminator (AHF110)	
407676691	120-VAC power-distribution unit (145D 6-AC)	
107949364	650A power supply	
848477634	LAN cross-over cable (RJ45), 12-foot	
405362641	120-VAC power cord	
106278062	Apparatus blank (circuit-pack blank) (158P)	

1 of 2

Table 3: Comcodes for equipment used with G600 ***2 of 2***

Comcode	Description	Optional
106606536	Integrated channel-service unit (ICSU) (120A2)	×
107988867	DS1 loop-back jack (T1 Only) (700A)	×
848477634	Cross-over cable	×
107152969	75-Ohm DS1 coaxial adapter (888B)	×
403613003	157B connecting block (“sneak-current protectors”)	×
406948976	6SCP-110 protector	×
107435091	507B sneak-current fuse panel	×
407216316	220029 sneak-current fuse	×
104307327	C6C cable – 50-foot (15.2-m) shielded DS1 cable with 50-pin male to 15-pin male	×
104307376	C6D cable – 50-foot (15.2-m) shielded DS1 cable with 50-pin male on each end	×
104307434	C6E cable – 100-foot (30.5-m) shielded DS1 cable with 50-pin male to 50-pin female	×
104307475	C6F cable – 50-foot (15.2-m) shielded DS1 cable with 50-pin male to 3-inch (7.62-cm) stub	×
102381779	3B1A carbon block	×
104410147	3B1E-W wide-gap gas tube	×
105514756	3C1S analog-line protector – solid state	×
102904893	4B1C carbon block with heat coil	×
104401856	4B1E-W wide-gap gas tube with heat coil	×
104386545	4C1S analog-line protector – solid state with heat coil	×
105581086	4C3S-75 digital voice-circuit protector – solid state	×
406144907	ITW Linx gas tube, avalanche suppress	×
901007120	ITW Linx ground bar (used with above)	×
406304816	ITW Linx replacement fuse	×
103972758	Data-link protector (1 circuit)	×
103972733	Data-link protector (8 circuits)	×
407063478	Electrostatic discharge (ESD) wrist strap	
407691401	Z3A2 alarm adapter (required with UPS)	×

2 of 2

Install and cable a G600 cabinet

WARNING:
Be sure there is adequate ventilation in the area. The internal room temperature must not exceed 50° C (122° F).

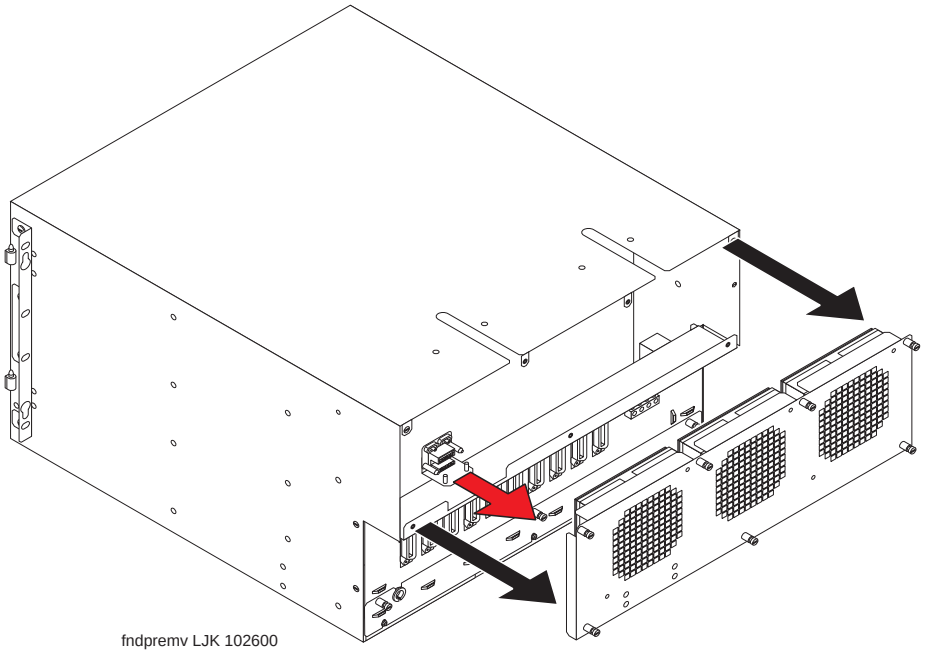
A G600 cabinet can be either floor- or rack-mounted. Set the Carrier Address ID either before or after installing each G600.

WARNING:
It is very important to align the cabinet with the correct holes in the frame because the distance between each varies. To aid your installation of the rack-mounted cabinet, **print** a copy of the G600 mounting template provided on this CD. Print the template on **11″× 17″**paper, so you can use it as an actual template.

Verify the carrier address ID on G600 cabinets

1 Loosen the thumb screws on the fan assembly and pull it straight out as shown in Figure 3, Fan assembly removal, on page 65.

Figure 3: Fan assembly removal



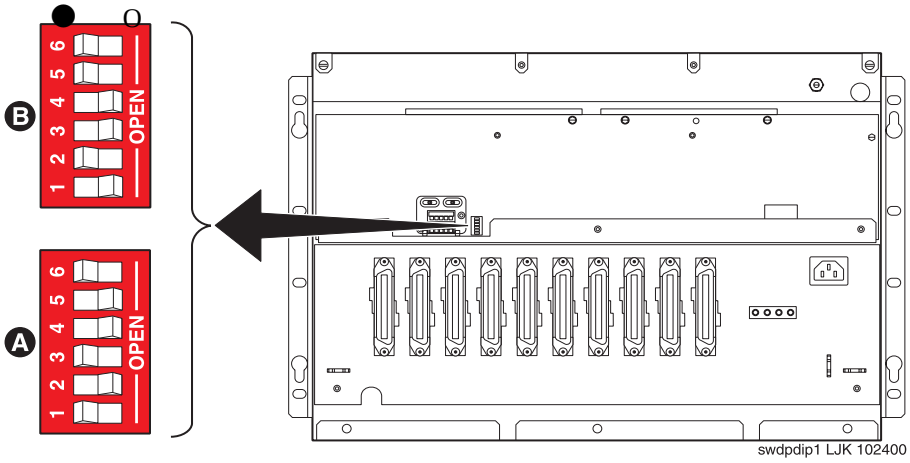
2 Verify and, if necessary, set the carrier address ID for each cabinet as shown in Table 4, Carrier address ID settings, on page 66 and Figure 4, Setting G600 carrier address ID, on page 66. Cabinet A is the processor cabinet, and Cabinets B, C, and D are optional port carrier cabinets. (S8100 supports up to three cabinets, A, B, and C.)

Table 4, Carrier address ID settings, on page 66 shows the settings for Cabinets A, B, C, and D. The **l**s and Os indicate closed and open positions, respectively, of the 6 rocker switches on the switch panel. For example, switches 2, 4, and 5 are in the closed position for Cabinet A. This table is embossed on the cabinet next the switch panel.

Table 4: Carrier address ID settings

	A	B	C	D
6	O	O	O	O
5	**l**	O	O	**l**
4	**l**	**l**	O	O
3	O	**l**	O	O
2	**l**	O	O	O
1	O	**l**	**l**	**l**

Figure 4: Setting G600 carrier address ID



3 Proceed to either Floor mount a G600 cabinet on page 67 or Rack mount a G600 cabinet on page 68.

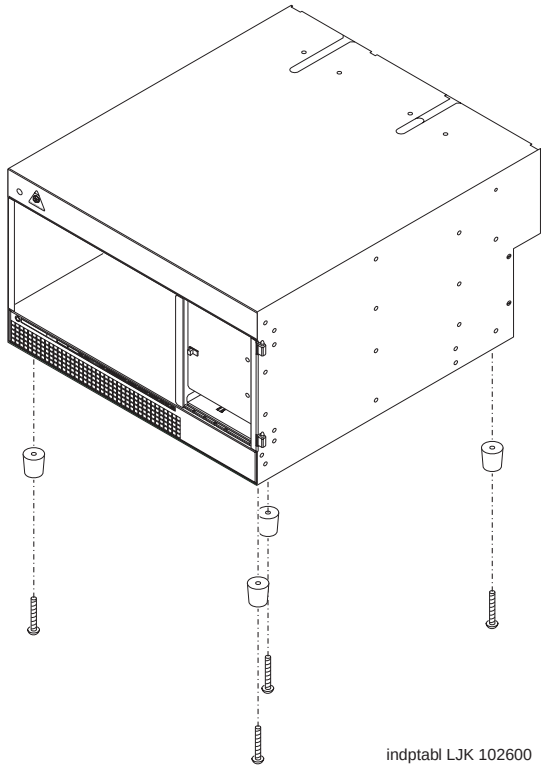
Floor mount a G600 cabinet

NOTE:
A single G600 can be either floor- or rack-mounted. Double and triple G600 systems must be rack-mounted.

WARNING:
Do not stack one G600 on top of another on the floor.

1 Screw the feet to the cabinet's base as shown in Figure 5, Floor-mounting the G600, on page 67.

Figure 5: Floor-mounting the G600



2 Locate the cabinet on the floor.

3 Proceed to Check AC power and ground for G600 on page 72.

Rack mount a G600 cabinet

WARNING:
Verify that the customer-supplied standard 19″rack is properly installed and solidly secured to the floor. If not, do not proceed with the installation.

1 Be sure the door has been removed.

2 Remove every circuit pack and the power supply.

WARNING:
When handling a circuit packs or any component of the G600, always wear an authorized wrist ground strap connected the ground connector provided on the system's cabinet. During a cabinet's installation, store circuit packs so that they will not be damaged by electrostatic discharge.

3 If necessary, prepare the G600 for mounting in the medial position by removing the screws on the mounting brackets, moving the brackets to a position midway on the cabinet, and installing the screws through the mounting bracket and into the cabinet's holes.

4 Using the rack-mounting guide, locate a set of rack holes to be used for mounting. Note the position of the upper key-hole shaped slots on each rail.

NOTE:
The mounting screws' holes are not evenly spaced on a 19″rack. Be sure the holes selected to mount a G600 are positioned to match every mounting-bracket slot on the guide. See Figure 6, Checking rack's mounting holes and placing first mounting screws, on page 69.

WARNING:
Installing the top G600 higher than shoulder level on the rack is not recommended.

5 Insert two mounting screws into the left and right rails of the rack in the holes noted in step 4. Leave enough space between the screw head and the rail surface to accept the mounting bracket. See Figure 6, Checking rack's mounting holes and placing first mounting screws, on page 69.

6 Lift the empty G600 and slide the key-hole slots on the mounting brackets onto the two mounting screws.

DANGER:
Use lifting precautions! An empty G600 weighs 15.8 – 17.6 kg (35 – 39 lbs).

Figure 6: Checking rack's mounting holes and placing first mounting screws

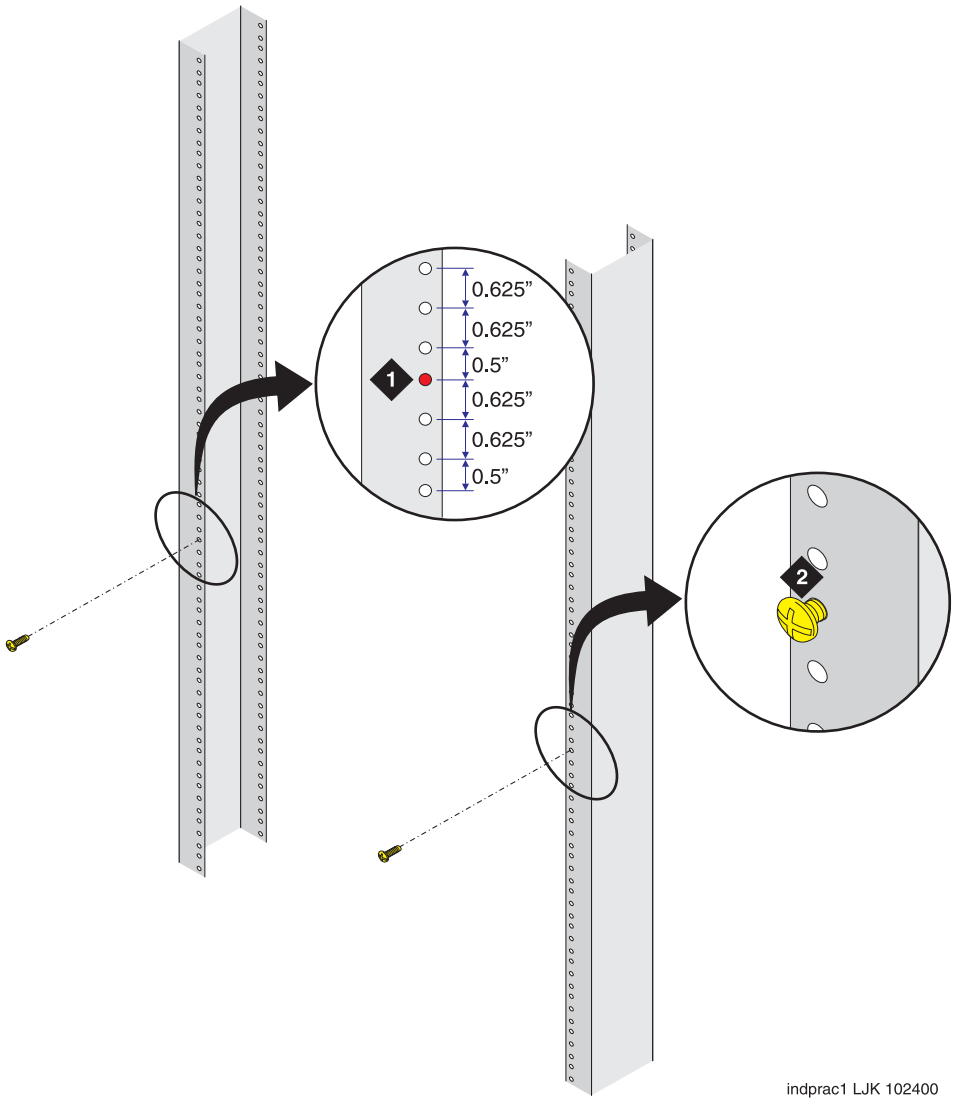
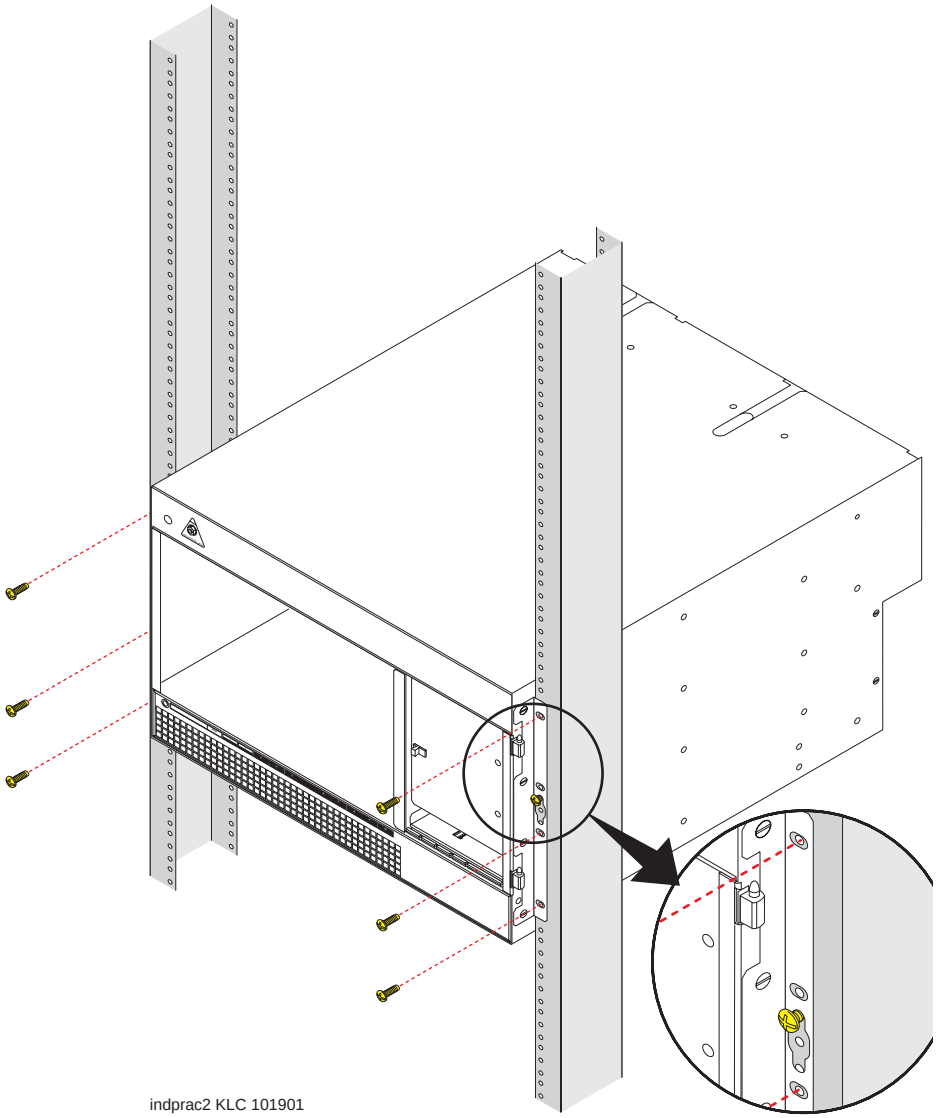


Figure notes

1 Spacing of rack's mounting holes

2 Mounting screw

Figure 7: Rack-mounting the G600

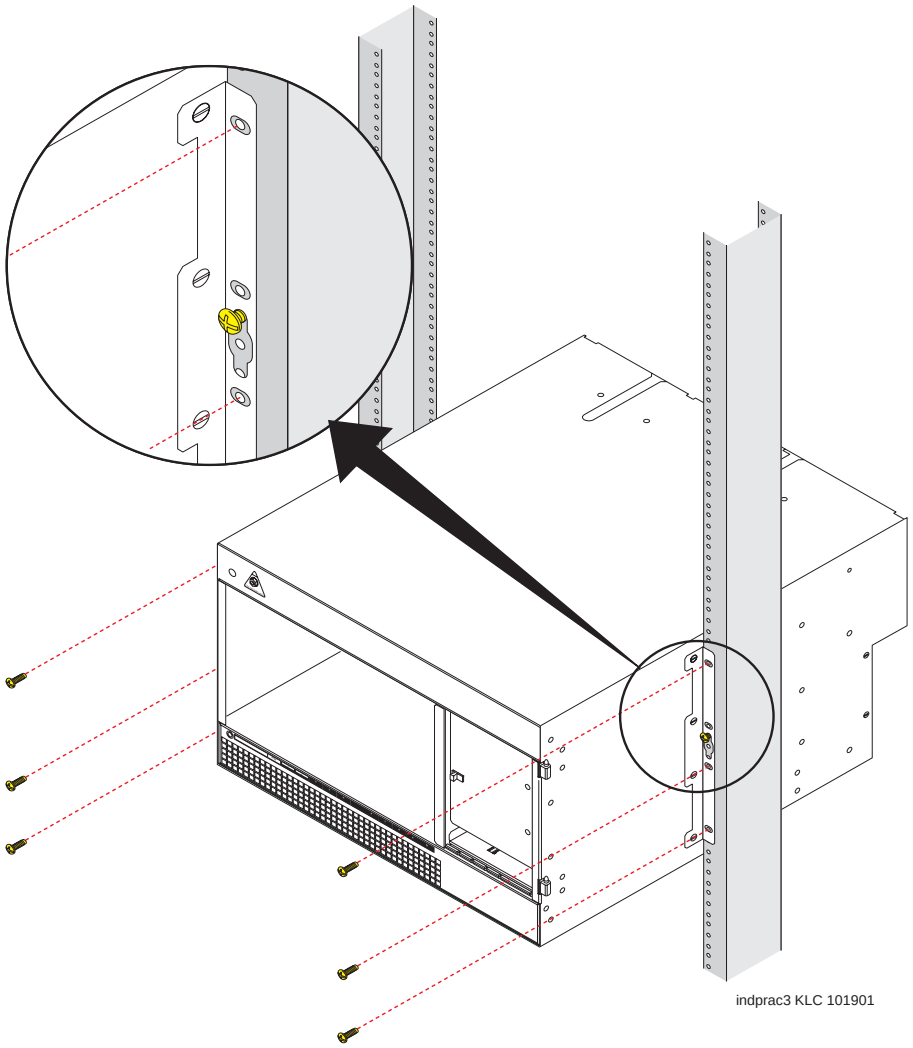


7 Tighten the two top mounting screws.

8 Install and tighten the remaining screws. See Figure 7, Rack-mounting the G600, on page 70.

NOTE:
Follow the same steps to install the G600 with mounting bracket in the medial position. See Figure 8, Rack-mounting the G600 in medial position., on page 71.

Figure 8: Rack-mounting the G600 in medial position.



9 Reinstall the circuit packs and power supply.

10 Proceed to Check AC power and ground for G600 on page 72.

Rack mount two G600 cabinets

Mount port Cabinet B directly above processor Cabinet A.

1 Install the rectangular EMI gasket over the right TDM-/LAN-bus cable routing slot on the top of Cabinet A. Be sure the open corner of the gasket faces the rear of the cabinet. Once installed, Cabinet B should rest on and compress the gasket. See Figure 14, Shift TDM-/LAN-bus terminator from Cabinet A to Cabinet B, on page 81.

2 Follow the steps to Rack mount a G600 cabinet on page 68.

3 Proceed to Check AC power and ground for G600 on page 72.

Check AC power and ground for G600

WARNING:

The alternating current (AC) power circuit ***must be*** dedicated to the system. The circuit ***must not be*** shared with other equipment and ***must not be*** controlled by a wall switch. The AC receptacle ***must not be*** located under the G600's main distribution frame and ***must be*** easily accessible.

DANGER:

The latch only removes the cabinet's direct current (DC) power. Unseating the power supply removes AC power from the power supply, but not from the cabinet. To remove the cabinet's AC power, pull the AC power cord from the AC appliance connector behind the cabinet.

WARNING:

System grounding ***must comply*** with the general rules for grounding provided in Article 250 of the National Electrical Code (NEC), National Fire Protection Agency (NFPA) 70, or the applicable electric code in the country of installation.

WARNING:

AC mains wiring and testing ***must be performed*** by a qualified electrician and ***must conform*** to Article 250 of the NEC, NFPA 70, or the applicable electric code in the country of installation.

WARNING:

Be sure that, with the other equipment installed in the rack, the G600 will not generate an overcurrent or over load condition. Verify that the customer's branch circuit and/or power-distribution strip are adequate with respect to overload and overcurrent protection.

Check AC power

Each G600 uses an auto-ranging (85 to 264 VAC) power supply, 47 to 63 Hz, 330 Watts, 4.5 Amps (100 to120 VAC) or 2.3 Amps (200 to 240 VAC), at 500 VoltAmps (VA).

The AC power source can be 1 phase of 120 VAC with neutral (100 VAC for Japan) with 15-Amp circuit breaker, or 1 phase of 220 or 240 VAC (200 VAC for Japan) with 10-Amp circuit breaker. The AC cord uses a NEMA 5-15P plug or an IEC 320 plug.

Before powering up the system, check the AC power in the equipment room using a KS-20599 digital voltmeter (DVM) (or equivalent).

To check AC power:

1. Measure the AC voltage between the hot and neutral sides of the receptacle.
2. Depending on the AC power source, verify that the meter reads 90 to 132 VAC or 180 to 264 VAC. If not, have a qualified electrician correct the problem.
3. Measure the voltage between the neutral and ground sides of the receptacle.

4 Verify that the meter reads 0 VAC. If not, have a qualified electrician correct the problem.

5 When finished, set the AC main circuit breakers to ***OFF***.

Approved grounds

An approved ground is the closest acceptable medium for grounding the building entrance protector, entrance cable shield, or single-point ground of electronic telephony equipment. If more than one type of approved ground is available on the premises, the grounds must be bonded together as required in Section 250-81 of the National Electrical Code.

WARNING:
Be sure that the G600 has a reliable earth ground connection, whether the G600 is connected directly to a branch circuit or to a power-distribution strip. In addition, the G600 requires a ground connection from the cabinet directly to an approved ground.

Grounded Building Steel – The metal frame of the building where it is effectively grounded by 1 of the following grounds: acceptable metallic water pipe, concrete-encased ground, or a ground ring.

Acceptable Water Pipe – A metal underground water pipe, at least ½ inch (1.3 cm) in diameter, in direct contact with the earth for at least 10 feet (3 m). The pipe must be electrically continuous (or made electrically continuous by bonding around insulated joints, plastic pipe, or plastic water meters) to the point where the protector ground wire connects. A metallic underground water pipe must be supplemented by the metal frame of the building, a concrete-encased ground, or a ground ring. If these grounds are not available, the water pipe ground can be supplemented by 1 of the following types of grounds:

- Other local metal underground systems or structures – Local underground structures such as tanks and piping systems
- Rod and pipe electrodes – A 5/8-inch (1.6-cm) solid rod or 3/4-inch (2-cm) conduit or pipe electrode driven to a minimum depth of 8 feet (2.4 m)
- Plate electrodes – Must have a minimum of 2 ft^2 (0.185 m^2) of metallic surface exposed to the exterior soil

Concrete Encased Ground – An electrode encased by at least 2 inches (5.1 cm) of concrete and located within and near the bottom of a concrete foundation or footing in direct contact with the earth. The electrode must be at least 20 feet (6.1 m) of 1 or more steel reinforcing bars or rods ½ inch (1.3 cm) in diameter, or at least 20 feet (6.1 m) of bare, solid copper, 4 AWG (26 mm^2) wire.

Ground Ring – A buried ground that encircles a building or structure at a depth of at least 2.5 feet (0.76 m) below the earth's surface. The ground ring must be at least 20 feet (6.1 m) of 2 AWG (35 mm^2), bare, copper wire.

Approved floor grounds

WARNING:
If the approved ground is inside a dedicated equipment room, these connections must be made by a qualified electrician.

Floor grounds are those grounds on each floor of a high-rise building that are suitable for connection to the ground terminal in the riser closet and to the cabinet's single-point ground terminal. Approved floor grounds may include:

- Building steel
- The grounding conductor for the secondary side of the power transformer feeding the floor
- Metallic water pipes
- Power-feed metallic conduit supplying panel boards on the floor
- A grounding point specifically provided in the building for the purpose

Uninterruptible power supply

A recommended uninterruptible power supply (UPS) may be used for power holdover. The type of UPS depends on the holdover requirements. Total holdover capacity varies depending on the UPS. The UPS must provide surge protection for the G600 cabinet.

CAUTION:
The major-alarm contacts should ***only*** be connected to a UPS that can indicate its backup power status. For most non-Avaya UPSs, you should not use the major external device leads. Using these leads for anything else could cause an SPE download.

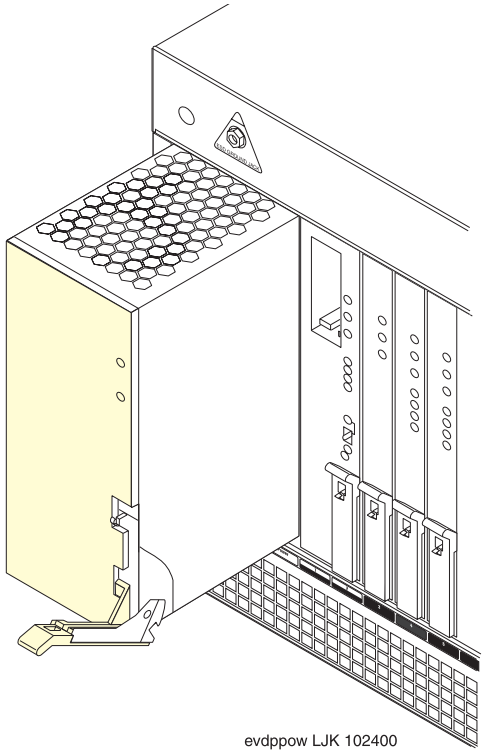
1. Connect the UPS to an electrical outlet capable of handling the power requirements of the cabinets:
   a. 100 VAC, 4.5 Amps
   b. 120 VAC, 3.8 Amps
   c. 200 VAC, 2.3 Amps
   d. 220 to 240 VAC, 2.0 Amps
2. Ensure that the cabinet is connected to an "unswitched" or "always-on" electrical outlet on the UPS.
3. For an Avaya UPS, connect and administer the UPS. See Connect external alarms and auxiliary connections on page 113.

NOTE:
If an Avaya UPS is wired as recommended, holdover time for each power outage is 1 minute before an automatic shutdown. UPS may handle any subsequent power outage based on its total battery capacity.

Cabinet's power switch

DANGER:
The latch acts as the DC power switch and only removes DC power from the cabinet, *not* AC power. To remove AC power, pull the AC power cord from the appliance inlet. See Figure 9, G600 650A power supply, on page 75.

Figure 9: G600 650A power supply



t

Connect cabinet's grounds and other grounds

Follow these additional grounding requirements:

- The approved ground wire must be green, 6 AWG (#40) (16 mm^2), copper, stranded wire. This is in addition to the ground wire in the AC power cord.
- Bond every approved ground at the single-point ground to form a single grounding electrode system.
- Connect the cable as shown in Figure 10, Single-cabinet G600 grounding, on page 76 for a single G600 cabinet, or Figure 11, 2-cabinet G600 grounding, on page 77 for two or three G600 cabinets.

Figure 10: Single-cabinet G600 grounding

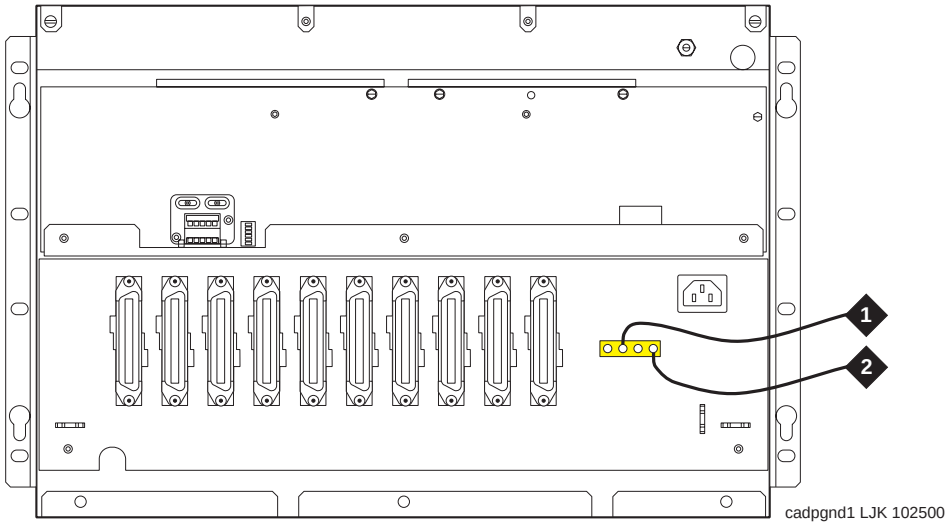


Figure notes

1 10 AWG (#25) (6 mm^2) wire to coupled bonding conductor (CBC).

2 6 AWG (#40) (16 mm^2) ground wire from single-point ground block to the approved building ground.

Figure 11: 2-cabinet G600 grounding

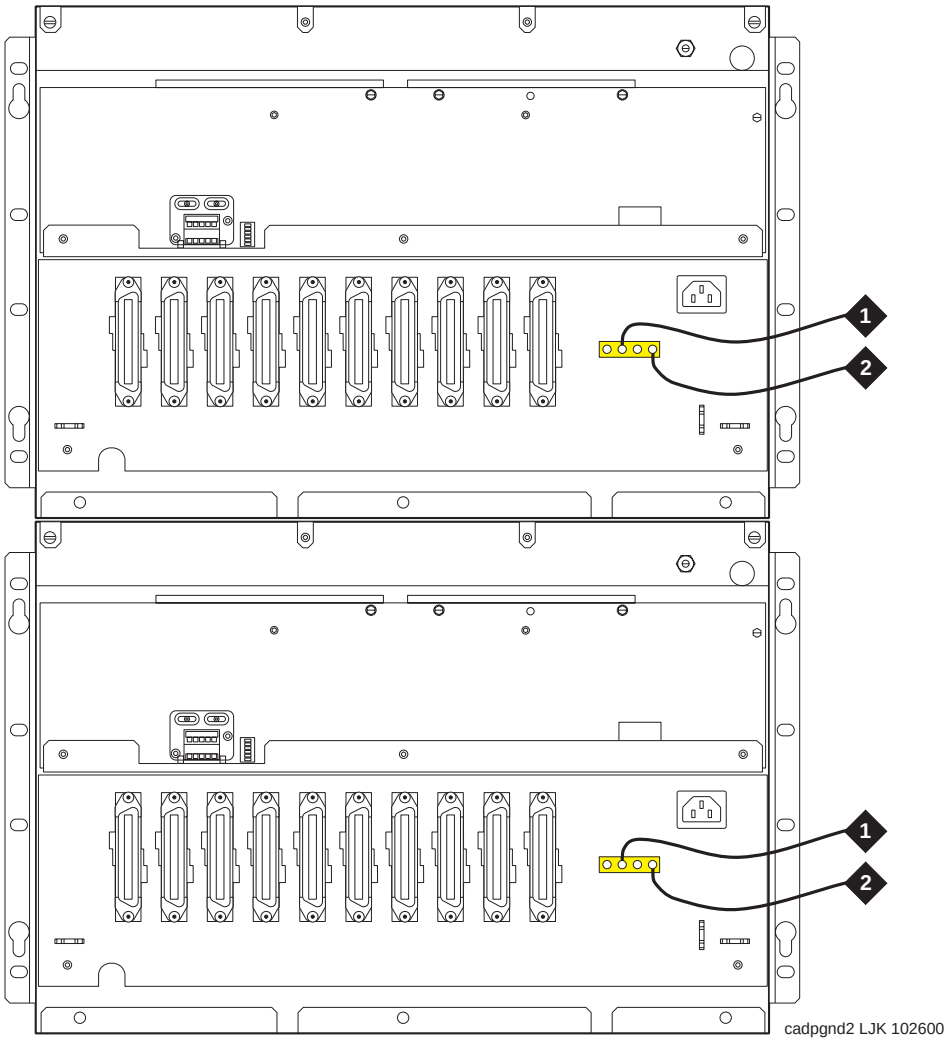


Figure notes

1 10 AWG (#25) (6 mm^2) wire to coupled bonding conductor (CBC)

2 6 AWG (#40) (16 mm^2) ground wire from single-point ground block to the approved building ground

Note: The grounding requirements for the 3rd cabinet in a 3-cabinet configuration are the same as for the 1- and 2-cabinet requirements.

Install coupled bonding conductor

The coupled bonding conductor (CBC) provides mutual inductance coupling between the CBC and the telephone cables exposed to lightning. The conductor can be a 10 AWG (#25) (6 mm^2) wire tie wrapped to the exposed cables, a metal cable shield around the exposed cables, or 6 spare pairs from the exposed cable.

For a high-rise building, connect the CBC to an approved building ground on each floor. To provide the coupled bonding protection:

1. Connect one end of the conductor to a telephone cable building entrance protector ground that is connected to an approved ground.
2. Route the conductor next to the exposed telephone cables being protected until it reaches the cross-connect nearest to the telephone system.
3. Position the unexposed telephone cables at least 12 inches (30.5 cm) away from exposed telephone cables whenever possible.
4. Terminate the other end to the single-point ground block provided for the telephone system.

Connect the power cords

WARNING:
The AC power cord may connect to a properly rated power-distribution unit, individual AC power receptacles, or to a UPS. A rack-mounted UPS is recommended.

To connect the power cords:

1. Ensure the AC load center's circuit breakers are ***OFF***.
2. Connect the cabinet to the UPS or to an "unswitched" or "always-on" electrical outlet.

Cable a G600 system

NOTE:
TDM-/LAN-bus terminators are factory installed on single G600 units. See Figure 12, Processor cabinet's TDM-/LAN-bus terminators, on page 79.

Figure 12: Processor cabinet's TDM-/LAN-bus terminators

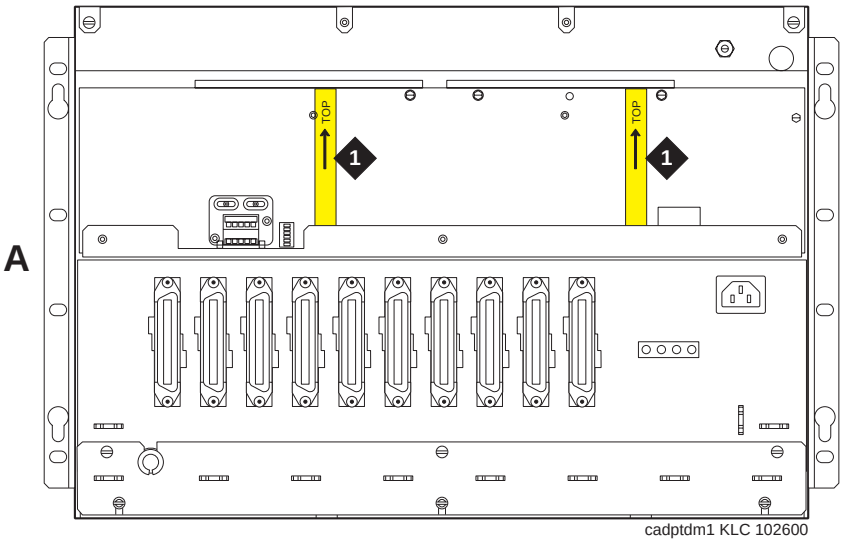


Figure notes

1 TDM-/LAN-bus terminators on the left and right TDM-/LAN-bus pin fields.

Install Processor Interface cable

1. Connect the Processor Interface cable to the slot 2 connector behind the processor cabinet. See Figure 13, G600 cable connections, on page 80.
2. Install the IP Media Processor adapter and 259A C-LAN adapter on the appropriate connectors behind the processor cabinet.
3. Install connector retainers.
4. Secure cables with tie-wraps for strain relief.

Figure 13: G600 cable connections

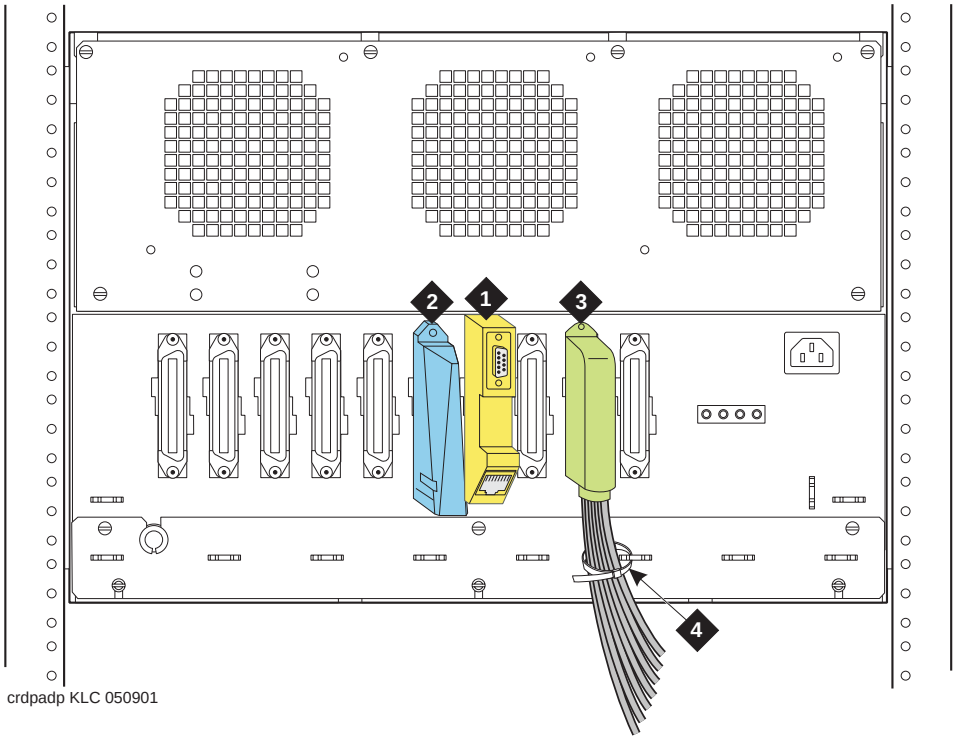


Figure notes

1	IP Media Processor adapter	**3**	Processor Interface cable (slot 2)
2	259A adapter for C-LAN	**4**	Tie-wrap anchor point

Cable a 2-cabinet G600 system

NOTE:
See Cable a 3-cabinet G600 system on page 84 for a 3-cabinet configuration.

1. Remove the bottom panel and fan assembly from Cabinet B (port cabinet).
2. Remove the fan assembly from Cabinet A (processor cabinet).
3. Remove the right TDM-/LAN-bus terminator from Cabinet A, and install it on the left TDM-/LAN-bus pin field on Cabinet B. See Figure 14, Shift TDM-/LAN-bus terminator from Cabinet A to Cabinet B, on page 81.

WARNING:
Be sure to install each TDM-/LAN-bus terminator with the arrow on its back pointing upward.

Figure 14: Shift TDM-/LAN-bus terminator from Cabinet A to Cabinet B

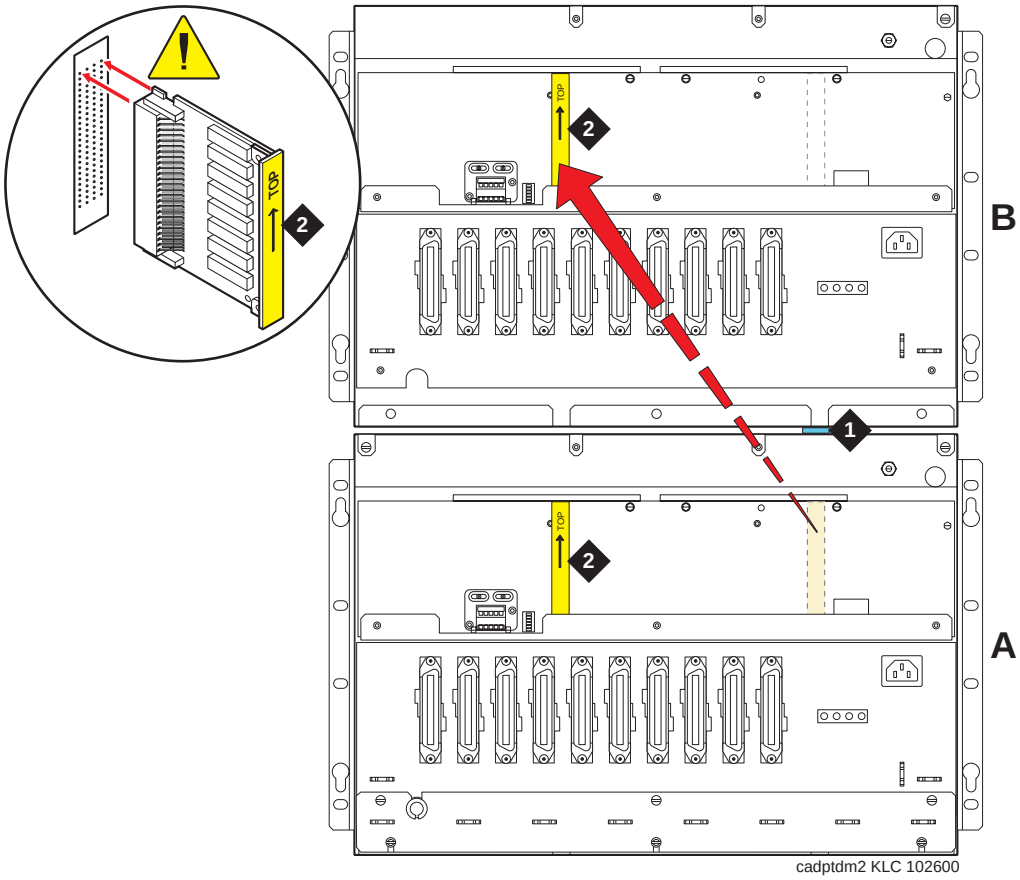


Figure notes

1	EMI gasket between cabinets	**2**	TDM-/LAN-bus terminators

4 Remove the nuts on the posts of the plates covering the bottom right TDM/LAN cable routing slot of Cabinet B and the top right TDM/LAN cable routing slot of Cabinet A. See Figure 15, TDM-/LAN-bus cable routing slot plate removal, on page 82

Figure 15: TDM-/LAN-bus cable routing slot plate removal

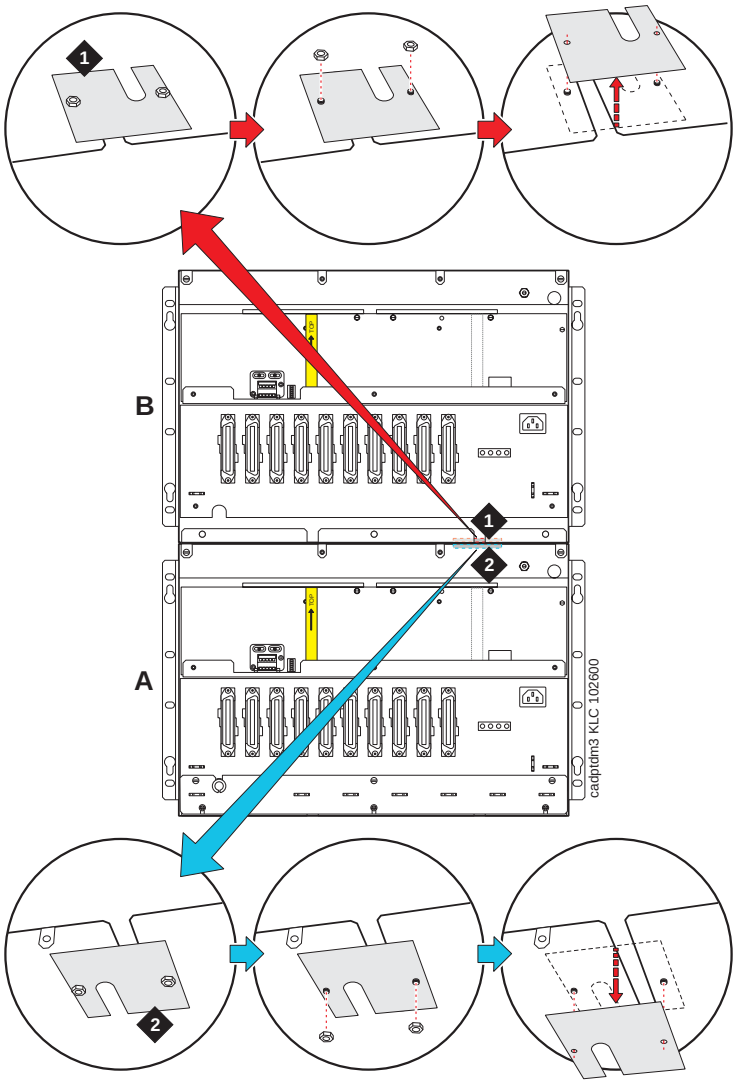


Figure notes

1 Cabinet B's routing slot plate. **2** Cabinet A's routing slot plate.

5 Pull open the EMI gasket, and pass the TDM-/LAN-bus cable through the routing slots in both cabinets. Push the free end of the EMI gasket back in place. See Figure 16, TDM-/LAN-bus cable routed from Cabinet A to Cabinet B, on page 83.

WARNING:
Be sure to install each TDM-/LAN-bus cable connector with the arrow on its back pointing upward.

6 Install the lower connector of the TDM-/LAN-bus cable on the right TDM-/LAN-bus pin field in Cabinet A.

7 Install the upper connector of the TDM-/LAN-bus cable on the right TDM-/LAN-bus pin field in Cabinet B.

8 Flip over the routing slot plates and reinstall both. Once the plates are reinstalled, the ends of the routing slots are covered.

9 Reinstall the fan assemblies and bottom panel.

Figure 16: TDM-/LAN-bus cable routed from Cabinet A to Cabinet B

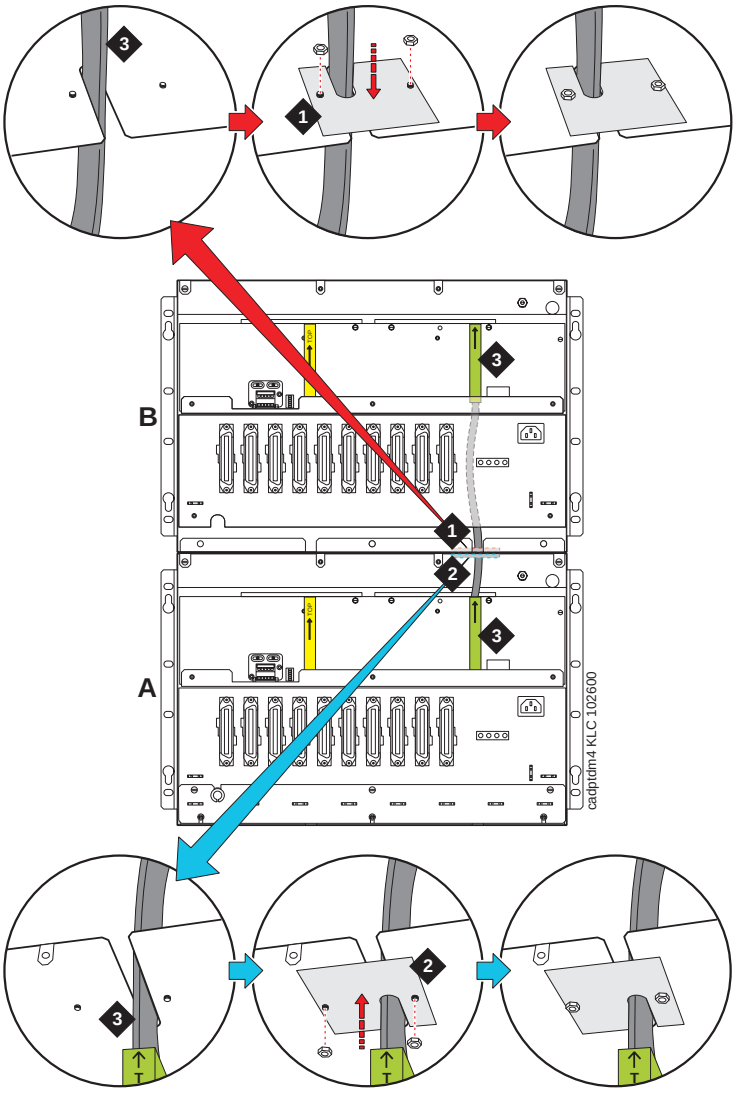


Figure notes

1 Cabinet B's routing slot plate, reversed

2 Cabinet A's routing slot plate, reversed

3 TDM-/LAN-bus cable

Cable a 3-cabinet G600 system

The procedure to connect the TDM-/LAN-bus cable for three cabinets is essentially the same as described in the previous section, Cable a 2-cabinet G600 system on page 80.

For three cabinets (A, B, and C), mount Cabinet A at the bottom, Cabinet B in the middle above A, and Cabinet C at the top above B. Between A and B, connect the TDM-/LAN-bus cable to the right pin field on both cabinets. Between B and C, connect the TDM-bus cable to the left pin field on both cabinets. The TDM-/LAN-bus terminators are installed on the left pin field on Cabinet A and on the right pin field on Cabinet C.

Install G600 patch panels and external modem

NOTE:
The optional patch-panel kit replaces standard 110A cross-connect hardware. If standard 110A cross-connect equipment is used, consult *DEFINITY Communications System Generic 1 and Generic 3 Main Distribution Field Design* (555-230-630).

Patch panels are arrays of RJ45 jacks and associated B25A cabling to accommodate 2-wire, 24-port DCP/analog port boards and 8-port analog trunk boards.

A shelf is provided to serve as a mounting surface for the external modem and other optional equipment. The shelf can also be used to secure the B25A cables.

Install patch panels and shelf

Refer to Figure 17, Typical G600's patch-panel and modem installation, on page 85 while performing this procedure.

1. Using the supplied mounting screws, mount the patch panels on the rack below processor cabinet.
2. Using the supplied mounting screws, mount the shelf on the rack below the patch panels.
3. Attach B25A cables to the patch panels and the circuit packs' amphenol connectors.

NOTE:
Connect 24-port DCP/Analog circuit packs to the 24-port patch panels.

NOTE:
Connect 8-port Analog Trunk, "combo," or DID Trunk circuit packs to either of the first two banks on the 8-port patch panel. If an 8-port BRI Trunk circuit pack (TN2185B) is present, connect it to the 3rd bank on the 8-port patch panel.

NOTE:
The patch panels do not have to be mounted in the same rack as the cabinet. They can be mounted in phone closets as appropriate.

Figure 17: Typical G600's patch-panel and modem installation

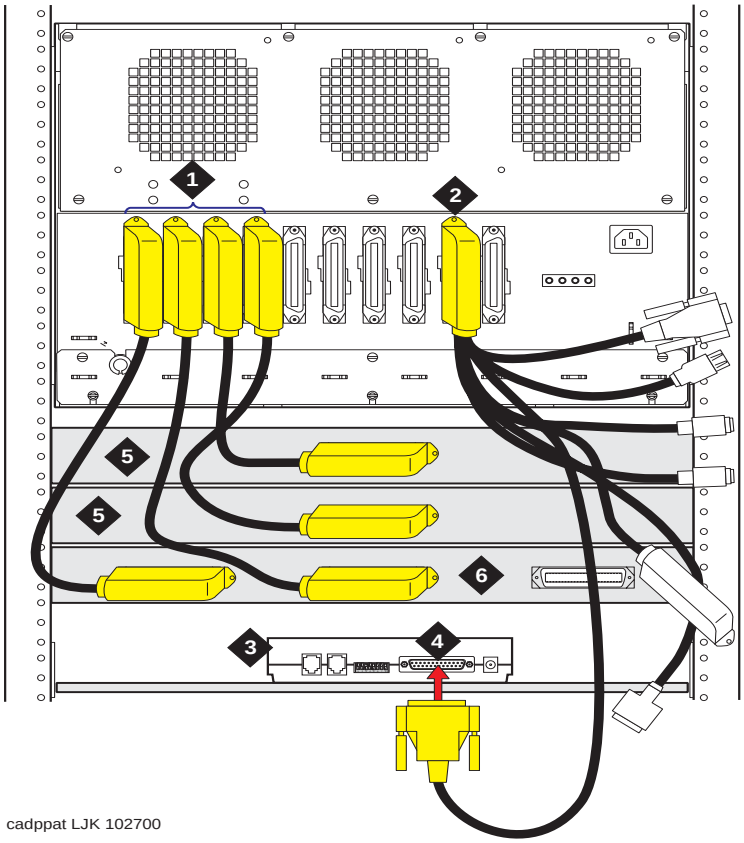


Figure notes

1	Circuit packs' amphenol connectors and B25A cables	**4**	P2 termination of Processor Interface cable attached to modem
2	Processor Interface cable	**5**	24-port patch panels
3	External modem (purchased separately)	**6**	8-port patch panel

Install the external modem

The US Robotics external modem is the recommended external modem. G600 systems operate with this modem set to factory default settings.

NOTE:
You may use a locally obtained, type-approved external modem (33.6 kbps or higher and V.34 protocol). Contact your Avaya representative for more information.

WARNING:
If you use a modem other than the US Robotics modem, it must be configured in Windows.

1. Securely mount the external modem at the left of the modem utility shelf or another secure surface.
2. Route the modem cable (P2) from the Processor Interface cable to the modem and attach it to the modem port.
3. Plug the modem power cord into the same power source as the G600(s), preferably the UPS.
4. Connect the modem to a standard analog line using RJ45 cord.

Modem's configuration and administration on page 262 describes information about modem setup, administration, settings, and testing.

Install equipment-room hardware for G600

See *DEFINITY Communications System Generic 1 and Generic 3 Main Distribution Field Design* (555-230-630) for more information.

Cross-connect the cabinet to the patch panels

1. Cross-connect the port circuit packs to the G600 patch panels (or other standard 110A cross-connect equipment). See Figure 19, Example cross-connect field's patch-panel connections, on page 93.

Allowed circuit packs

Table 5, Allowed circuit packs and circuit modules, on page 86 lists the circuit packs that can be used with G600. (Table 6, Disallowed circuit packs and circuit modules, on page 89 lists the circuit packs that cannot be used with G600.)

Table 5: Allowed circuit packs and circuit modules ***1 of 3***

Apparatus code	Name	Allowed?
650A	AC power unit	Yes
NAA1	Fiber-Optic Cable Adapter circuit pack	Yes
TN417	Auxiliary Trunk	Yes
TN429/B/C/D	Analog Direct Inward/Outward Dialing (DIOD) Central Office Trunk	Yes
TN429C	Analog Central Office Trunk	Yes
TN429D	Analog DIOD Trunk – Analog Loop Start	Yes
TN433	Speech Synthesizer	Yes
TN436B	Direct Inward Dialing Trunk	Yes
TN437B	Tie Trunk Australia (future availability)	Yes

1 of 3

Table 5: Allowed circuit packs and circuit modules ***2 of 3***

Apparatus code	Name	Allowed?
TN438B	Central Office Trunk	Yes
TN439	Tie Trunk	Yes
TN447	Central Office Trunk	Yes
TN457	Speech Synthesizer	Yes
TN459B	Direct Inward Dialing Trunk	Yes
TN464GP	DS1 Interface – T1, 24 Channel - E1, 32 Channel	Yes
TN465B/C	Central Office Trunk	Yes
TN467	Analog Line	Yes
TN468B	Analog Line	Yes
TN479	Analog Line	Yes
TN553	Packet Data Line	Yes
TN556C/D	Integrated Services Digital Network -Basic Rate Interface 4-Wire S/T-NT Interface (ISDN-BRI)	Yes
TN722B	DS1 Tie Trunk	Yes
TN725B	Speech Synthesizer	Yes
TN726B	Data Line	Yes
TN735	Multibutton Electronic Telephone (MET) Line	Yes
TN742	Analog Line	Yes
TN744E	Call Classifier – Detector	Yes
TN746B	Analog Line	Yes
TN747/B	Central Office Trunk	Yes
TN750C	Announcement	Yes
TN753/B	Direct Inward Dialing Trunk	Yes
TN754/B/C	Digital Line 4-Wire DCP	Yes
TN758	Pooled Modem	Yes
TN760B/C/D/E	Tie Trunk	Yes
TN762/B	Hybrid Line	Yes
TN763B/C/D	Auxiliary Trunk	Yes
TN767B/C/D/E	DS1 Interface – T1, 24 Channel	Yes
TN769	Analog Line	Yes
TN771/D	Maintenance/Test	Yes

2 of 3

Table 5: Allowed circuit packs and circuit modules ***3 of 3***

Apparatus code	Name	Allowed?
TN789	Radio Controller	Yes
TN791	Analog Line	Yes
TN793	Analog Line, 24-Port, 2-Wire	Yes
TN2314	Processor	Yes
TN799DP	Control LAN (C-LAN)	Yes
TN802/B	Internet Protocol (IP) Trunk	Yes
TN2135	Analog Line	Yes
TN2136	Digital Line 2-Wire DCP	Yes
TN2138	Central Office Trunk	Yes
TN2139	Direct Inward Dialing Trunk	Yes
TN2140B	Tie Trunk – Hungary, Italy	Yes
TN2144	Analog Line	Yes
TN2146	Direct Inward Dialing Trunk	Yes
TN2147C	Central Office Trunk	Yes
TN2149	Analog Line	Yes
TN2180	Analog Line	Yes
TN2181	Digital Line 2-Wire DCP	Yes
TN2183	Analog Line	Yes
TN2184	DIOD Trunk	Yes
TN2185/B	ISDN-BRI 4-Wire S/T-TE Interface (Trunk Side)	Yes
TN2199	Central Office Trunk	Yes
TN2207	DS1 Interface – (T1) 24 Channel and (E1) 32 Channel	Yes
TN2224/B	Digital Line, 24-Port, 2-Wire DCP	Yes
TN2242	TTC Japanese 2Mbit Trunk	Yes
TN2302	IP Media Processor	Yes
TN2305	Asynchronous Transfer Mode (ATM) Trunk	Yes
TN2464	DS1 Interface – T1, 24 Channel - E1, 32 Channel	Yes
TN2793/B	Analog Line 24-Port	Yes

3 of 3

Disallowed circuit packs

Table 6, Disallowed circuit packs and circuit modules, on page 89 lists the circuit packs that cannot be used with G600.

Table 6: Disallowed circuit packs and circuit modules ***1 of 2***

Apparatus code	Name	Allowed?
982LS	Current Limiter	No
CFY1B	Current Limiter	No
CPP1	Memory Expansion	No
ED-1E546 (TN566) (TN567)	INTUITY AUDIX R3 System	No
ED-1E546 (TN2208) (TN2170)	CallVisor Adjunct-Switch Application Interface (ASAI) over the DEFINITY LAN Gateway R1	No
J58890M-1 (TN801)	CallVisor ASAI/Call Visor PC/LAN over the DEFINITY LAN Gateway Release 2.0	No
TN419B	Tone-Clock	No
TN420B/C	Tone Detector	No
TN568	INTUITY AUDIX Slim	No
TN570B/C	Expansion Interface	No
TN572	Switch Node Clock	No
TN573B	Switch Node Interface	No
TN574	DS1 Converter – T1, 24 Channel	No
TN577	Packet Gateway	No
TN748B/C/D	Tone Detector	No
TN750B	Announcement	No
TN755/B	Neon power unit	No
TN756	Tone Detector/Generator	No
TN765	Processor Interface	No
TN768	Tone-Clock	No
TN772	Duplication Interface	No
TN775/B/C	Maintenance	No

1 of 2

Table 6: Disallowed circuit packs and circuit modules ***2 of 2***

Apparatus code	Name	Allowed?
TN776	Expansion Interface	No
TN777B	Network Control	No
TN778	Packet Control	No
TN780	Tone-Clock	No
TN787F/G/H/J/K	Multimedia Interface	No
TN788B	Multimedia Voice Conditioner	No
TN790B	Processor	No
TN792	Duplication Interface	No
TN794	Network Control/Packet Interface (NetPkt)	No
TN798B	Processor	No
TN801	LAN Gateway Interface	No
TN1648/B	System Access/Maintenance	No
TN1650B	Memory	No
TN1654	DS1 Converter – T1, 24 Channel/E1, 32 Channel	No
TN1655	Packet Interface	No
TN1656	Tape Drive	No
TN1657	Disk Drive	No
TN2182/B	Tone-Clock – Tone Detector and Call Classifier	No
TN2198	ISDN-BRI 2-Wire U Interface	No
TN2202	Ring Generator	No
TN2210	Tone Generator	No
TN2214/B	Digital Line, 24-Port, 2-Wire DCP – Category B only	No
TN2215	Analog Line, 16-Port 2-Wire – Category B only	No
TN2238	ATM Trunk Interface (multimode)	No
TN2301	Survivable Remote Logic Switch	No
TN2306	ATM Interface (single-mode)	No
TN2308	Direct Inward Dialing Trunk	No

2 of 2

Circuit-pack installation

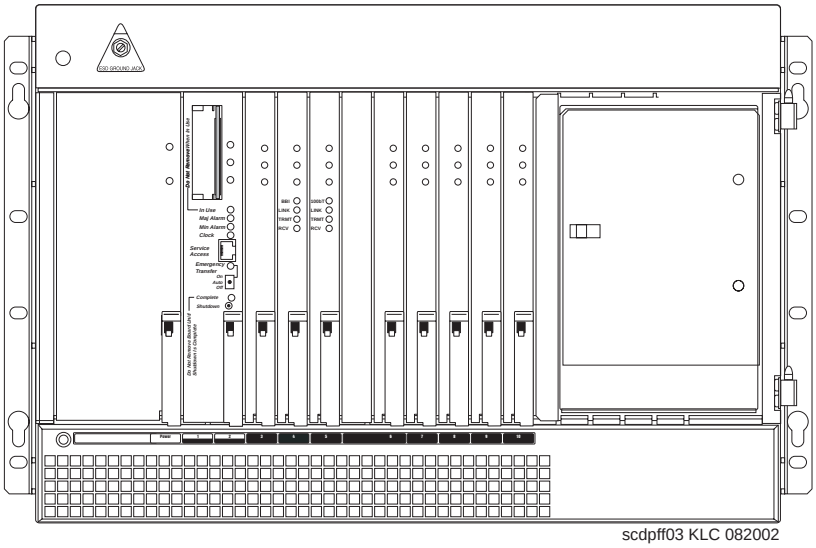
WARNING:

When handling a circuit pack or any component of a G600 system, always wear an authorized wrist ground strap. Connect the strap to the ground connector provided on the system's cabinet.

Circuit-pack slot loading

1. Check the reinstalled circuit packs. Every circuit-pack slot in the G600 is a "universal slot." Any slot can contain any type of port circuit pack with the following exceptions for Cabinet A. See Figure 18, G600 cabinet and slot numbering, on page 91.
   - TN2314 Processor circuit pack must be installed in slot 2 of Cabinet A.
   - TN744E Call Classifier/Tone Detector circuit pack should be installed in slot 3.
2. Load every port circuit pack. See Table 7, Circuit-pack installation order (loading), on page 91 for the recommended circuit-pack layout.

Figure 18: G600 cabinet and slot numbering



scdpff03 KLC 082002

Table 7: Circuit-pack installation order (loading) ***1 of 2***

Function	Apparatus code	Load G600 from	Notes
Processor	TN2314	Slots 1 and 2	
Call Classifier/Tone Detector	TN744E	Slot 3	
Announcement	TN750C	Any slot	
Speech Synthesizer	TN725B	Any slot	
Control C-LAN	TN799DP	Left	

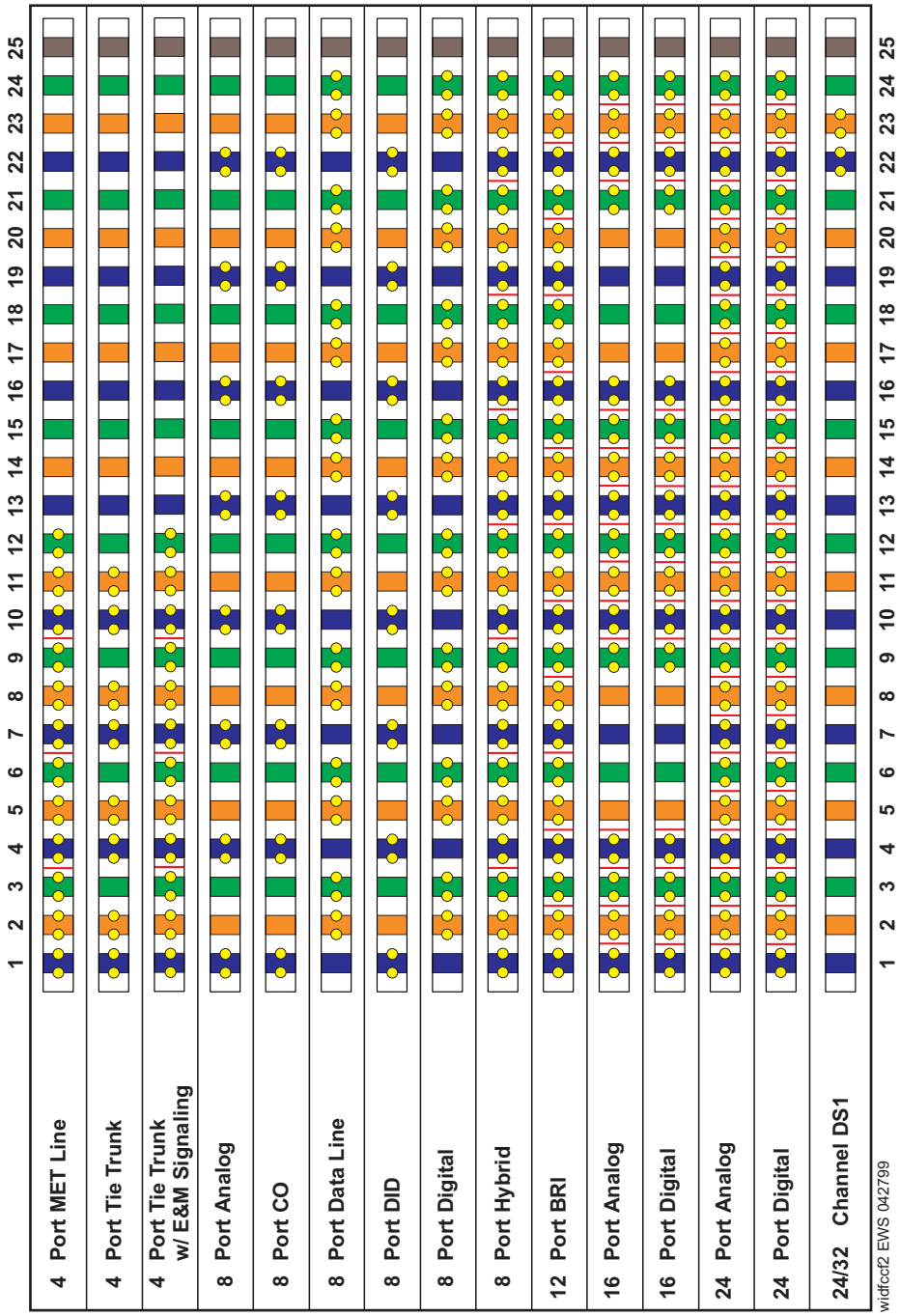
1 of 2

Table 7: Circuit-pack installation order (loading) ***2 of 2***

Function	Apparatus code	Load G600 from	Notes
Media Processor	TN2302	Left	
DS1/E1, ISDN-PRI	TN464GP, TN767E, TN2242, TN2464	Left	Maximum of 7 – Total number of ISDN-PRI **and** ISDN-BRI circuit packs must not exceed 7.
ISDN-BRI Trunk	TN2185	Left	Maximum of 4
CO Trunk	TN747B, TN465C, TN2199, TN2147C, TN2138, TN438B	Left	
DID Trunk	TN753, TN2139, TN2146, TN436B, TN459B	Left	
Tie Trunk	TN760E, TN458, TN497, TN2140B	Left	
Auxiliary Trunk	TN417	Left	
Modem Pool	TN758	Left	
Data Line	TN726	Right	
Digital Line	TN754C, TN2181, TN2224/B	Right	
Analog Line	TN746B, TN2135, TN467, TN2144, TN2149, TN2180, TN2183, TN2215, TN468B,TN791, TN793, TN2793, TN2214	Right	
Hybrid Line	TN762B	Right	
MET Line	TN735	Right	
Radio Controller	TN789	Right	
ISDN-BRI 4-Wire S/T-NT Line (A-Law)	TN556C/D TN744E	Right	

2 of 2

Figure 19: Example cross-connect field's patch-panel connections



Off-premises circuit protection

Protection from hazardous voltages and currents is required for every off-premises (out-of-building) trunk, line, or terminal installation. Both over-voltage protection (lightning, power induction, and so forth) and sneak-current protection are required. Sneak-current protectors must be either UL-listed or CSA-certified, or must comply with local safety standards.

Sneak-current protectors must have a maximum rating of 350 mA and a minimum voltage rating of 600V, or as required by local regulations. The following devices protect the system from over-voltages:

- Analog trunks use the 507B sneak protector or equivalent. Over-voltage protection is normally provided by the local telephone company.
- Analog voice terminals use one of the following types of combined over-voltage and sneak-current protection, or equivalent:
  - — Carbon block with heat coil for UL code 4B1C
  - — Gas tube with heat coil for UL code 4B1E-W
  - — Solid state with heat coil for UL code 4C1S
- DCP and ISDN-BRI terminals use the solid state 4C3S-75 with heat coil protector, or equivalent.
- DS1/T1 circuits require isolation from exposed facilities. This isolation may be provided by a channel-service unit (CSU) (T1), or other equipment that provides equivalent protection.

Install sneak fuse panels

Sneak-current protection is required between the incoming RJ21X or RJ2GX network interface and the system for both trunk and off-premises circuit packs. The model 507B sneak-current fuse panel, or equivalent, is recommended for sneak-current protection. See Figure 20, Model 507B sneak fuse panel, on page 94.

Figure 20: Model 507B sneak fuse panel

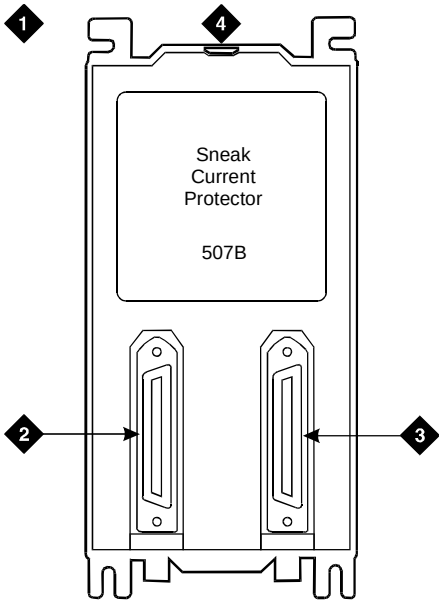


Figure notes

1	507B sneak-current protector (comcode 107435091)	**3**	25-pair female connector (out) (comcode 846300994)
2	25-pair male connector (in) (comcode 846300994)	**4**	220029 fuses (inside panel) – Use a small screwdriver to pry top cover off.

Each column of sneak fuse panels requires approximately 8 inches (20 cm) of horizontal wall space. Connector cables connect the network interface to the sneak fuse panel. Also, use 157B connecting blocks equipped with SCP-110 protectors for sneak-current protection.

NOTE:
Sneak-current protectors with a rating of 350 mA at 600 V must be UL-listed for United States installations or CSA-certified for Canadian installations. The panel contains 2 25-pair connectors, fuse removal tool, and fifty 220029 sneak fuses (and 2 spares). Use the SCP-110 protectors with 110-type hardware and on the 507B sneak fuse panel. The SCP-110 protectors can be ordered separately and installed on the 157B connecting block. Fifty protectors are required per block.

1 Install the 507B near the network interface or patch panels with locally-obtained #12 × ¾-inch screws (or equivalent).

Table 8, Sneak fuse connector pinout, on page 95 is a pinout of the cable wiring and associated fuse numbers.

Table 8: Sneak fuse connector pinout ***1 of 2***

Connector Pin Numbers	Pair/Fuse Number
26/1	1
27/2	2
28/3	3
29/4	4
30/5	5
31/6	6
32/7	7
33/8	8
34/9	9
35/10	10
36/11	11
37/12	12
38/13	13
39/14	14
40/15	15
41/16	16
42/17	17

1 of 2

Table 8: Sneak fuse connector pinout ***2 of 2***

Connector Pin Numbers	Pair/Fuse Number
43/18	18
44/19	19
45/20	20
46/21	21
47/22	22
48/23	23
49/34	24
50/25	25
	2 of 2

Set ringing option for G600

Figure 21: Selection of ringing option

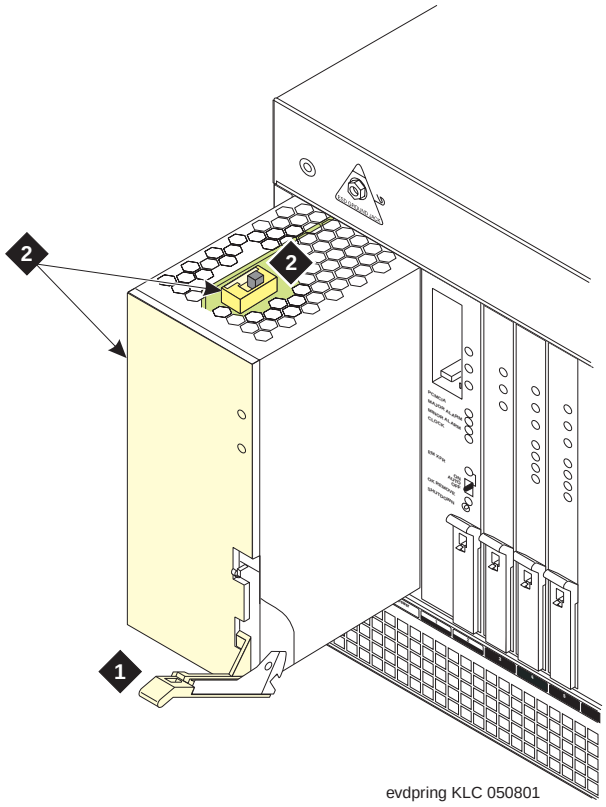


Figure notes

1 Attachment lever

2 Ringing option switch and setting label

NOTE:
Look at the label on the side of the power supply to see how to set the switch.

Figure 22: TN2314 circuit pack's faceplate

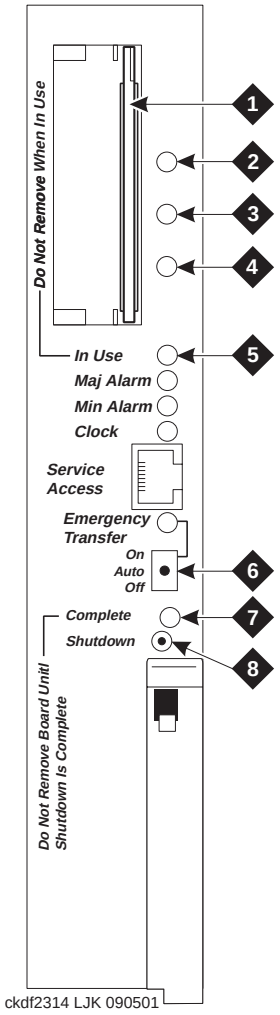


Figure notes

1	PCMCIA slots	**5**	PCMCIA in-use LED
2	Red LED	**6**	Emergency Transfer switch
3	Green LED	**7**	Shutdown-complete LED – Safe to pull board when green LED is on
4	Amber LED	**8**	Shut-down switch – Gracefully shuts down system

Section II – Install telephones and make auxiliary connections

This section describes procedures for installing and wiring telephones and making auxiliary connections.

Install and wire telephones and other equipment

NOTE:
Only 1 pair of wires is available for emergency transfer, and 1 pair of wires is available for attendant console power.

The wiring procedures are similar for most Avaya telephones and other equipment. This section provides wiring examples for similar installation procedures. Actual wiring procedures may vary at each site.

The system can connect to any DTE terminal. The system can have RS-232 (or EIA-232) or DCP interfaces.

As necessary, following sections of this chapter provide wiring pinouts for various port circuit packs. Also, Table 47, Leads for circuit packs and auxiliary equipment (pinout charts), on page 281 has pinout information for every port circuit pack.

Punch-down information for common circuit packs is in Figure 73, Example MDF connections, on page 380. This figure shows the colors of the punch-downs and is best viewed from CD-ROM or on-line.

After installing the hardware, the data for the system and telephone features can be administered. These procedures are provided in *Administrator's Guide for Avaya Communication Manager* (555-233-506).

Telephone connection examples

The 302C1 attendant console (AC) describes a typical telephone connection. This information is typical of the 603E, 84xx (4-wire), and 94xx telephones. The AC always requires auxiliary (adjunct) power (-48 VDC). See Figure 23, Wiring 302C1 to a Digital Line circuit pack, on page 100. Only 1 console can be powered by the system through the auxiliary (AUX) connector. The primary console should be powered from the system so it has the same power failure backup as the system.

The maximum cabling distance for a cabinet-powered console is 350 feet (100 meters) using 24-AWG (#5) (0.26-mm^2) wire.

The general steps to connect a telephone are:

1. Choose a device to connect, such as a 302C1 attendant console.
2. Choose the port circuit pack, its carrier, and slot number (such as TN754C, Carrier A, Slot 06).
3. Choose a port circuit on the port circuit pack, such as Port 05.
4. Install cross-connect jumpers to wire the terminal to the port circuit pack. See Figure 23, Wiring 302C1 to a Digital Line circuit pack, on page 100. This pinout is for a 4-wire Digital Line circuit pack.

Figure 23: Wiring 302C1 to a Digital Line circuit pack

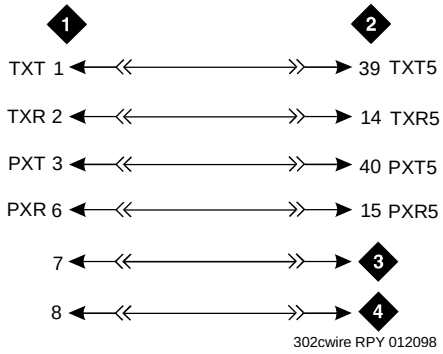


Figure notes

1	302C1 attendant console	**3**	-48 VDC from adjunct power
2	4-wire Digital Line circuit pack	**4**	Ground from adjunct power

Connect adjunct power

The400B2 adapter is convenient for connecting local -48 VDC power to a modular plug. See Figure 24, 400B2 adapter connecting to a modular plug, on page 100.

Figure 24: 400B2 adapter connecting to a modular plug

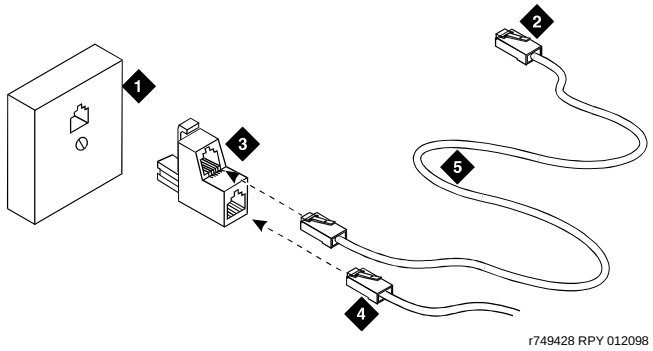


Figure notes

1	Surface-mounted information outlet	**4**	To telephone
2	To individual power unit (such as 1151B or 1151B2)	**5**	Destination service access point (DSAP) power cord
3	400B2 adapter		

Adjunct power can be provided from the equipment room or equipment closet with 1145B power unit. The AUX connector (J1) on the Processor Interface cable can provide power for 1 attendant console.

Adjunct power can be provided locally at the telephone or console by the 1151B or 1151B2 power supply.

Station wiring examples

This section shows the wiring connections for the various types of stations. See Figure 25, Typical station wiring connections, on page 101, Table 9, Wiring color code, on page 102, and Table 10, Stations connections, on page 102.

Figure 25: Typical station wiring connections

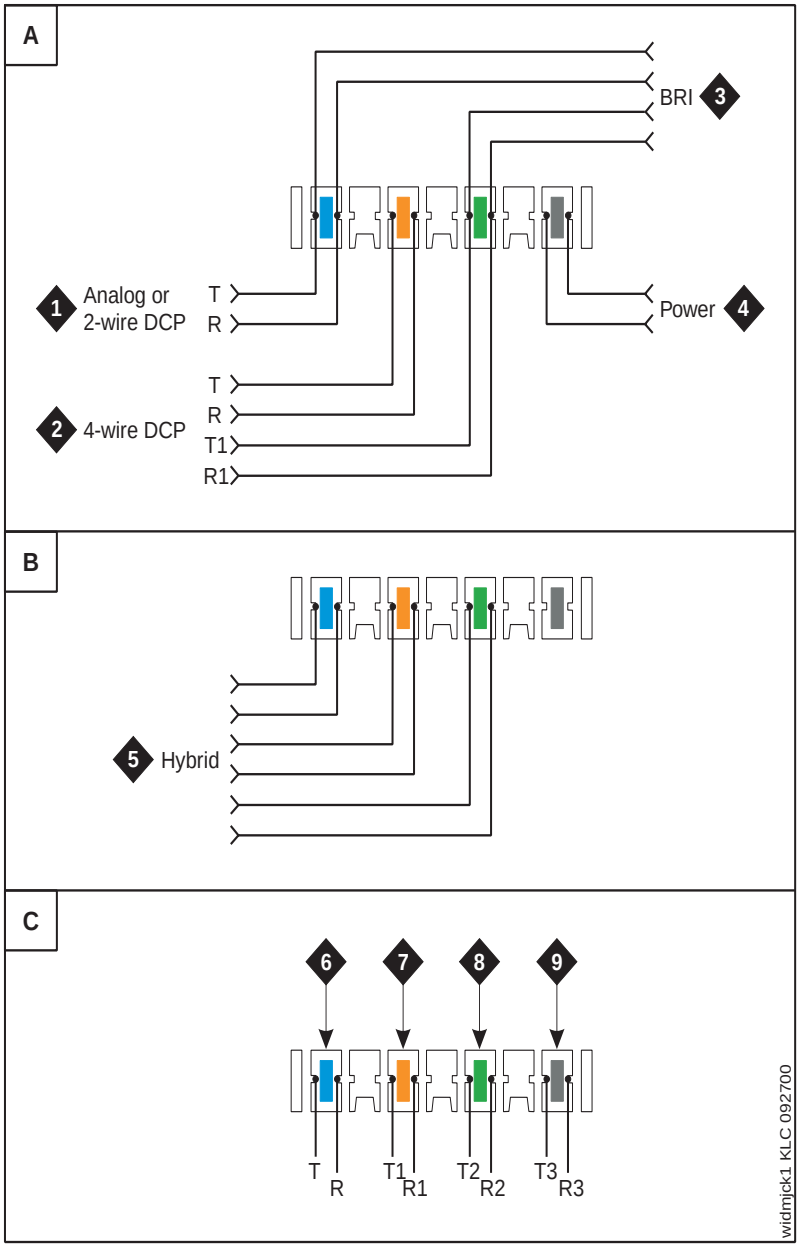


Table 9: Wiring color code

Station type	Wire color (tip/ring)
Analog	yellow/blue
2-wire DCP	white/orange
4-wire DCP	red/blue red/orange
Hybrid	white/blue white/orange white/green
Power	white/red

Table 10: Stations connections

Station type	Connector
Analog or 2-wire DCP	T=1, R=26
BRI	T=1, R=26 T1=3, R1=28
4-wire DCP	T=2, R=27 T1=3, R1=28
Hybrid	T=1, R=26 T1=2, R1=27 T2=3, R2=28
Power	4, 29

Analog tie trunk example

Figure 26: Analog tie trunk cross-connect

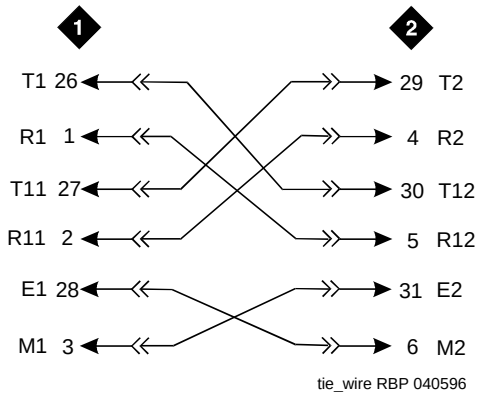


Figure notes

1	External trunk or adapter	**2**	Tie Trunk circuit pack

1. Before installing the Tie Trunk circuit pack, set the option switches as described in TN760E option-switch settings and administration on page 268.
2. Install cross-connect jumpers to connect the pins from the Tie Trunk circuit pack to the appropriate leads on the external tie trunk. Determine names of the tie trunk leads from the manufacturer or supplier of the external trunk circuit. The example in Figure 26, Analog tie trunk cross-connect, on page 103 shows an external tie trunk connected to a DS1 Interface circuit pack.
3. Administer on the Trunk Group form. See *Administrator's Guide for Avaya Communication Manager* (555-233-506).

Digital tie trunk example

Figure 27: Digital tie trunk wiring

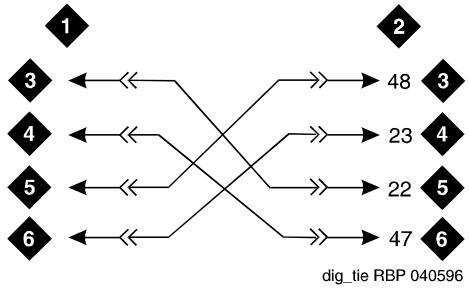


Figure notes

1	External trunk	**4**	LO (balanced output pair)
2	DS1 Interface circuit pack, position 1CA06	**5**	LI
3	LO	**6**	LI (balanced input pair)

1. Before installing the DS1 Interface circuit pack, set the option switches as shown in Set TN464GP T1/E1's options on page 269.
2. Install cross-connect jumpers to connect the pins from the digital trunk circuit pack to appropriate pins on the external digital trunk.
3. Administer the DS1 Interface circuit pack on the DS1 and Trunk Group screens. See *Administrator's Guide for Avaya Communication Manager* (555-233-506).

Cable examples for tie trunk connectivity

DS1 tie trunks provide 1.544-Mbps (T1) or 2.048-Mbps (E1) digital data service between 2 collocated systems or between the system and a data network. The following cables can be used:

- **C6C connector cable** – 50-foot (15.2-m) shielded cable with a 50-pin male connector on 1 end and a 15-pin male connector on the other end. Use to connect a DS1 Tie Trunk circuit pack to a channel-service unit.
- **C6D connector cable** – 50-foot (15.2-m) shielded cable with a 50-pin male connector on each end. Use to connect DS1 tie trunks in collocated cabinets.
- **C6E connector cable** – 100-foot (30.5-m) shielded cable with a 50-pin male connector on 1 end and a 50-pin female connector on the other end. Use as an "extension" cable between the DS1 Tie Trunk circuit pack and other connector cables.
- **C6F connector cable** – 50-foot (15.2-m) shielded cable with a 50-pin male connector on 1 end and a 3 inch (7.62-cm) stub on the other end. Use to connect the DS1 Tie Trunk circuit pack to channel multiplexers requiring hardwired connections. See Table 11, Pinout of C6F cable, on page 104 for a pinout.

Table 11: Pinout of C6F cable

Wire color	Lead designation	Pin number
White/Green	LI (high side)	47
Green	LI	22
White/Brown	LO	48
Brown	LO (high side)	23
White/Slate	LBACK2	49
Slate	LBACK1	24

DS1 tie trunks between collocated systems

Two DS1 Tie Trunk circuit packs can exist in collocated systems. A DS1 Tie Trunk circuit pack in 1 system can connect to a DS1 tie trunk in another system. Use a C6D cable if the distance is less than 50 feet (15.24 m). If the distance is greater than 50 feet (15.24 m), use a C6E cable.

NOTE:
The maximum distance between cabinets is 1310 feet (399 m).

DS1 tie trunks using T1 channel-service unit

Figure 28, Typical connections to channel-service unit, on page 105 shows a DS1 tie trunk connected to an external T1 channel-service unit (CSU). An enhanced 120A2 integrated channel-service unit (ICSU) can be used in place of an external T1 CSU. The CSU or ICSU interfaces the DS1 tie trunks with the 1.544-Mbps digital facility. Contact your Avaya representative for maximum cabling distances.

Figure 28: Typical connections to channel-service unit

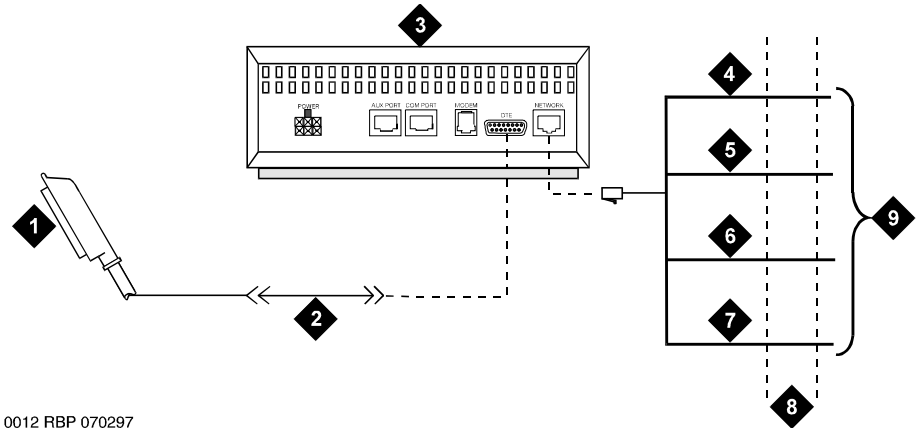


Figure notes

1	To DS1 Tie Trunk circuit pack	**5**	Ring (R)
2	C6C cable – If distance is over 50 feet (15.24 m), use C6E cable.	**6**	Tip 1 (T1)
		7	Ring1 (R1)
3	External T1 CSU or 120A2 ICSU	**8**	1.544-Mbps T1 interface
4	Tip (T)	**9**	To T1 carrier

3- and 4-pair modularity

Figure 29, 3- and 4-pair modularity, on page 106 shows 3- and 4-pair modularity from the port circuit pack to the voice or data terminal. Most terminals connect to an information outlet (modular jack) installed at the work location.

Figure 29: 3- and 4-pair modularity

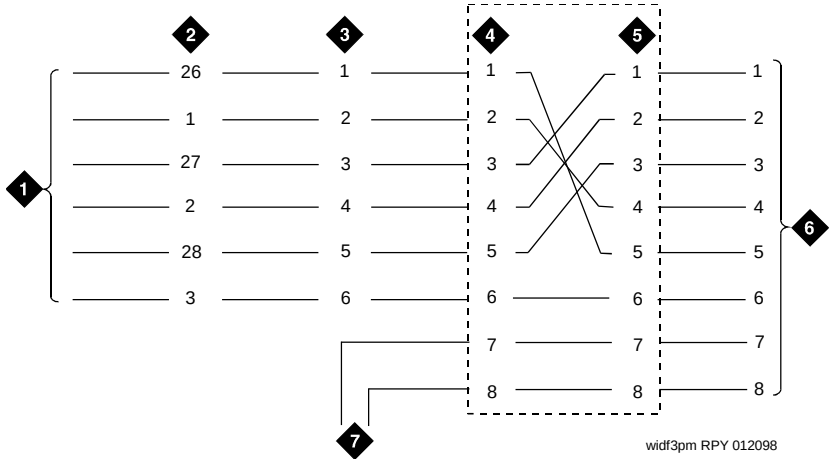


Figure notes

1 Port circuit pack

2 25-pair connector pins (3-pair modularity)

3 MDF pins (3-pair modularity)

4 Input to information outlet (4-pair modularity)

5 Output from information outlet (4-pair modularity)

6 Voice or data terminal pins

7 Adjunct power

Adjunct power connections

Figure 30, Example adjunct power connections, on page 107 shows typical connection locations for adjunct power.

Figure 30: Example adjunct power connections

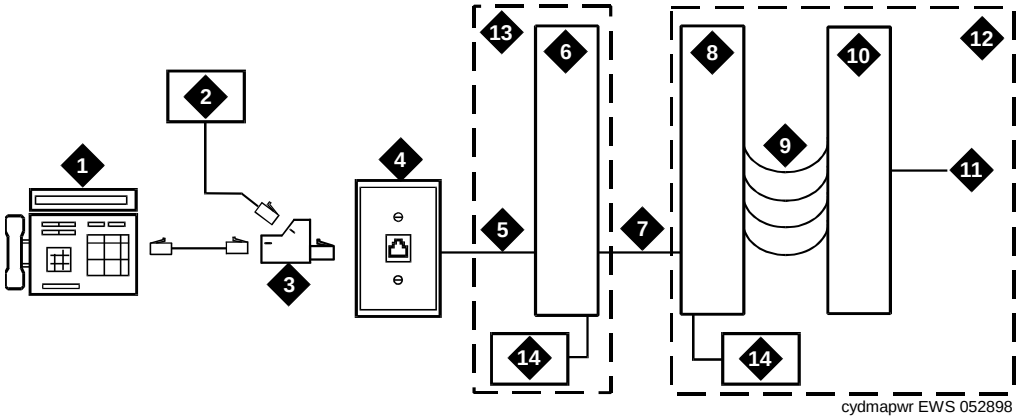


Figure notes

1 Typical display telephone

2 Individual power supply (such as 1151B, not used if item 14 is used)

3 400B2 adapter

4 Information outlet (modular jack)

5 4-pair D-Inside Wire (DIW) cable

6 Satellite site or adapter location

7 25-pair D-Inside Wire (DIW) cable

8 Station side of MDF or patch panel

9 100P6A patch cord or jumpers

10 System side of MDF or patch panel

11 25-pair cable to Digital Line circuit pack

12 Equipment room

13 Satellite location

14 Bulk power supply (such as 1145B). Install at satellite location or equipment room (not both).

Local and phantom power

The attendant console's (AC'c) maximum distance from the system is limited.
See Table 12, Attendant console cabling distances, on page 107.

Table 12: Attendant console cabling distances

Enhanced attendant console (302C1)	24 AWG wire (0.26 mm^2)		26 AWG wire (0.14 mm^2)	
	Feet	Meters	Feet	Meters
With selector console				
Phantom powered	800	244	500	152
Locally powered	5000	1524	3400	1037
Without selector console				
Phantom powered	1400	427	900	274
Locally powered	5000	1524	3400	1037

Auxiliary power

The nonessential functions of an AC and its optional 26A1 or 24A1 selector console derive power from an auxiliary power source. During short power outages, provide auxiliary power for an AC through this cable so the console remains fully operational.

NOTE:
Only 1 console can derive auxiliary power from the system and through the auxiliary cable located in the trunk/auxiliary field.

A console's maximum distance from its auxiliary power source is:

- 800 feet (244 m) for a 302A1
- 350 feet (107 m) for a 301B1 and 302C1

An AC can also derive auxiliary power from:

- Individual 1151B or 1151B2 power supply
- MSP-1 power supply
- 258A-type adapters
- Bulk power supplies such as the 1145A1

Install attendant console – optional

To install the optional AC:

1. Position the attendant console in the desired location and connect the modular cord to the information outlet.
2. Install labels according to assignments on the Attendant Console and Display Module forms.
3. Install a Digital Line circuit pack in the assigned carrier slot (if required).
4. Administer the console forms in *Administrator's Guide for Avaya Communication Manager* (555-233-506).

Hard-wire bridging

WARNING:
Bridging or paralleling these endpoints can cause *electrical damage to the consoles or cause the circuit pack to remove power from the consoles.*

Analog type hard-wire bridging is not allowed for 4-wire (only) DCP endpoints, because hard-wire bridging provides no way of combining the digital output of 2 bridged DCP sets. Also, a bridged endpoint causes the added load to degrade the DCP signal.

Dual wiring of 2-wire and 4-wire endpoints

Do not simultaneously wire a 2-wire and 4-wire endpoint to the same equipment location in an MDF, even though they connect to different colored wire pairs. The system uses separate circuit packs to interface 2- and 4-wire endpoints, and none are capable of interfacing both.

Install 26B1 selector console – optional

To install the optional selector console:

1. Connect the supplied 3-foot (0.9 m) D8AC cable to the modular jack on the bottom of the 26B1 selector console.
2. Route the cable to the attendant console and connect to the DXS/BLF jack.
3. Attach labels according to the Attendant Console form.
4. Administer the attendant console using *Administrator's Guide for Avaya Communication Manager* (555-233-506).

1152A1 Mid-Span power-distribution unit

The 1152A1 Mid-Span power-distribution unit (PDU) is an Ethernet power supply that provides power to up to 24 46xx-series IP telephones or wireless LAN (WLAN) access points. This unit is used with a 10/100BaseTx standard Ethernet network over a standard TIA/EIA-568 Category 5, 6 or 6e cabling plant. The 1152A1 meets the current requirements of the IEEE802.3af standard for resistive detection.

The 1152A1 PDU complies with the Underwriters' Laboratories, Inc. (UL) standard UL 1950, 2nd edition.

Table 13: 1152A1 PDU UL 1950 compliance

Complies	UL 1950
Approved	CSA C22.2 No.950 Std.
Approved	CE Regulatory Compliance
Approved	EN 60950
Approved	TUV EN 60950

For safety instructions, see Important safety instructions on page 109. For installation instructions, see Connect the cables on page 111.

Important safety instructions

Please read the following helpful tips. Retain these tips for later use.

When using this switch, the following safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons.

- Read and understand every instruction.
- Follow every warning and instruction marked on the switch.
- This product can be hazardous if immersed in water. To avoid the possibility of electrical shock, do not use it near water.
- The 1152A1 PDU contains components sensitive to electrostatic discharge. Do not touch the circuit boards unless instructed to do so.

- This product should be operated only from the type of AC (and optional DC) power source indicated on the label. If you are not sure of the type of AC power being provided, contact a qualified service person.
- Do not allow anything to rest on the power cord. Do not locate this product where the cord can be damaged by persons walking on it.
- Do not overload wall outlets and extension cords as this can result in the risk of line or electric shock.
- Disconnect the cords on this product and refer servicing to qualified service personnel under the following conditions:
  - If the power supply cord or plug is damaged or frayed.
  - If liquid has been spilled into it.
  - If it has been exposed to rain or water.
  - If it was dropped or the housing has been damaged.
  - If it exhibits a distinct change in performance.
  - If it does not operate normally when following the operating instructions.

Using the 1152A1 PDU

The 1152A1 PDU is used to power the 46xx series of IP telephones in addition to providing a 10-/100-Mbps Ethernet connection.

Generation 1 Avaya IP telephones can receive power from the 1152A1 via an in-line adapter. This adapter provides the resistive signature so that the 1152A1 allows power to flow to the telephone. The generation 2 telephones do not need an adapter.

The 1152A1 PDU has 24, 10/100 Base-T ports, each can supply up to 16.8 Watts using the internal power supply and operates on a 100- to 240-Volt AC, 60-/50-Hertz power source.

The 1152A1 PDU is 1µ high and fits in most standard 19-inch racks. It can also be mounted on a shelf. Refer to the user's guide that comes with the unit for complete installation instructions.

Connect the 1152A1 PDU

CAUTION:
The 1152A1 PDU has no ON/OFF switch. To connect or disconnect power to the 1152A1 PDU, simply insert or remove the power cable from the AC power receptacle behind the 1152A1 PDU.

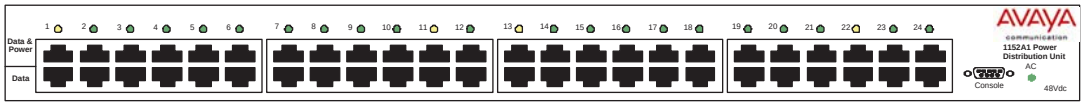
1. Plug a power cord into the power socket behind the 1152A1 power-distribution unit.
2. Plug the other end of the power cord into the power receptacle.

   The 1152A1 PDU powers up, and the internal fans begin operating.

The 1152A1 PDU then runs through its Power On Self Test (POST), which takes less than 10 seconds. During the test, every port on the unit is disabled and the LEDs light up. For more information about the test, refer to the user's guide that comes with the unit.

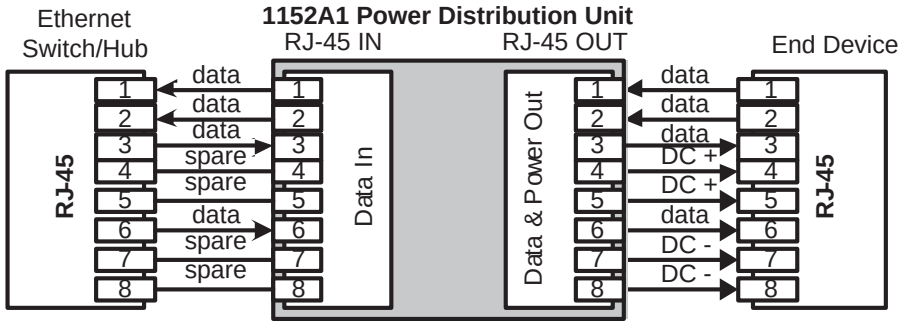
Connect the cables

Every port on the front of the 1152A1 PDU is configured as a data route-through port for every data wire (pins 1, 2, 3, and 6).



Use a standard CAT5, CAT6, or CAT6e straight-through Ethernet cable (not supplied), including all 8 wires (4 pairs) as shown in Connecting cables to telephones and other end devices on page 111.

Figure 31: Connecting telephones and other end devices to the 1152A1 PDU



For Data-In ports connect the Ethernet cable leading from the Ethernet Switch/Hub to the Data port. For Data & Power Out ports connect the Ethernet cable leading to the telephone or other end device to the corresponding Data & Power port.

NOTE:
Be certain to connect correspondingly numbered Data and Data & Power ports.

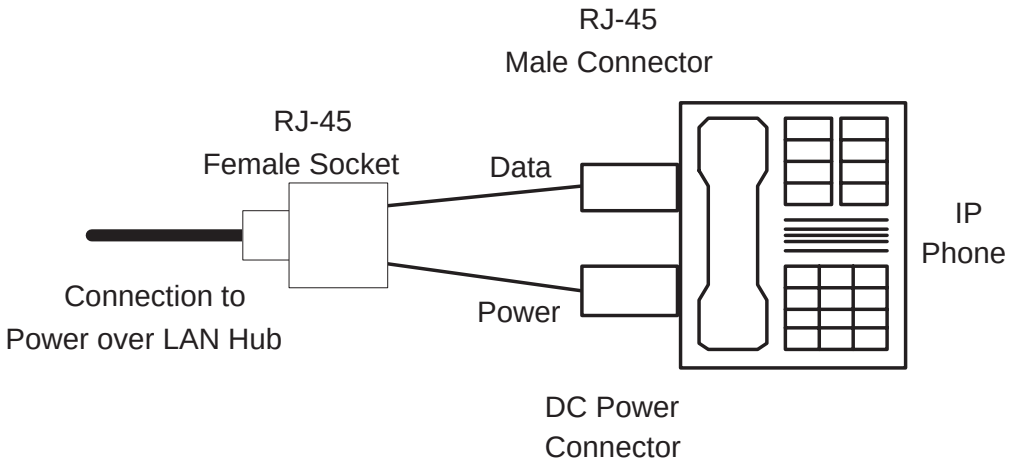
Connecting cables to telephones and other end devices

Due to an 1152A1 PDU's line-sensing capabilities, this PDU only powers end devices designed to receive power from the LAN. When connected to an 1152A1 PDU, such a device (termed Power over LAN Enabled) receives both its power and data via the Ethernet cable.

To safeguard devices that are not enabled, an 1152A1 PDU can detect these devices and send them data via the Ethernet cable, without transmitting power.

An end device that cannot receive power directly may receive its power and data through an external splitter. The splitter separates the power and data before connecting to the end device (see Connecting an IP telephone with an external splitter on page 112).

Figure 32: Connecting an IP telephone with an external splitter



Before connecting telephones or other end devices to the 1152A1 PDU, determine if

- It is Power over LAN Enabled or not.

  If not, you may safely connect the telephone; however, the port supplies no power and functions as a normal Ethernet data port.

- It requires an external splitter or whether it requires only a single RJ45 connection.

  If an external splitter is needed, be certain to use a splitter with the correct connector and polarity.

- It's power requirements are consistent with the 1152A1 PDU voltage and power ratings. Refer to Appendix B in the user's guide that comes with the unit for voltage and power ratings.

To connect telephones and other end devices to the 1152A1 PDU:

1. Connect an Ethernet cable to the telephone using an external splitter or directly (if the device is Power over LAN Enabled).
2. Connect the opposite end of the same cable to the RJ45 wall outlet.
3. On the front panel of the 1152A1 PDU, monitor the response of the corresponding port LED. If it lights up GREEN, the unit has identified your telephone as a Power over LAN

Connect external alarms and auxiliary connections

NOTE:
The AUX connector is part of the Processor Interface cable assembly (J1). When the wiring and administration are complete, give these wiring records to the Customer System Administrator for troubleshooting purposes.

Alarm input

Alarms can be generated on adjunct equipment, sent to the S8100 system, and recorded and reported as "external alarms."

CAUTION:
Pins 26 and 1 on the AUX connector are dedicated to the UPS alarm input. Using these pins for other alarm inputs will cause the S8100 system to reset.

1 Connect 1 major alarm *input* wire pair and 1 minor alarm *input* wire pair to the auxiliary field from the AUX connector (J1 on Processor Interface cable). See Table 14, Alarm inputs at AUX connector, on page 113 and Figure 33, UPS connection to G600 or CMC1, on page 114.

Table 14: Alarm inputs at AUX connector

Alarm input type	Color	AUX connector
Major (UPS)	White-Blue Blue-White	AP2 (Pin 27) Ground (Pin 2)
Minor	White-Orange Orange-White	AP2 (Pin 26) Ground (Pin 1)

Alarm output

The system provides a relay contact closure that can operate a customer-provided alarm, such as a light or bell. The customer provides the circuitry and power source. The alarm device must not exceed a rating of more than 30 VAC RMS or 60 VDC at 0.75 Amps.

To connect alarm output:

1 Connect the external alarm *output*. See Table 15, Alarm output at AUX connector, on page 114.

2 Type **change system-parameters maintenance** and press ENTER.

3 Change the CPE Alarm Activation Level field to the desired alarm level and press ENTER.

Table 15: Alarm output at AUX connector

Alarm output type	Color	AUX connector
EXTALMA	Violet-Green	(Pin 48)
EXTALMB	Green-Violet	(Pin 23)

UPS alarm connection

Figure 33: UPS connection to G600 or CMC1

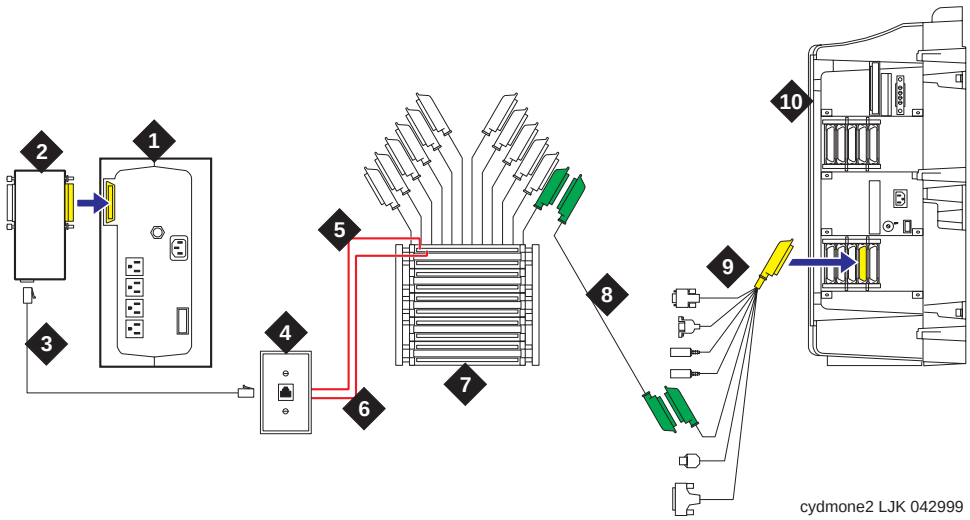


Figure notes

1	Avaya UPS	**6**	Pin 1, orange-white
2	Z3A2 alarm adapter	**7**	Cross-connect field
3	RJ45 (D8W) cable	**8**	25-pair cable
4	103A or modular jack	**9**	Processor Interface cable (AUX connector)
5	Pin 26, white-orange	**10**	G600 or CMC1

Emergency transfer and auxiliary power

NOTE:
Only 1 emergency transfer power panel and 1 auxiliary power connection are provided per system.

Connect emergency transfer power and auxiliary power as shown in Table 16, Emergency transfer and auxiliary power, on page 115. Auxiliary power includes power to an attendant console or adjunct device.

Table 16: Emergency transfer and auxiliary power

Power type	Color	AUX connector
Emergency Transfer	Black-Blue Blue-Black	XFER48 (Pin 36) Ground (Pin 46)
Adjunct -48 VDC	Brown-Yellow Yellow-Brown	ACC48A (Pin 19) Ground (Pin 44)

Telephone pin designations

Table 17, Port circuit pack and telephone pin designations, on page 115 provides pack and pin designations.

Table 17: Port circuit pack and telephone pin designations

Pin on modular plug	4-wire; 302C1, 8400-series, 603E, 9403, 9434	2-wire; 302C1, 8400-series, 603E, 9403, 9410, 9434	8510T BRI (with adjunct speaker phone)	Analog station, modem	Z3A1 & Z3A2 ADU, data module
1	TXT				TXT
2	TXR			T	TXR
3	PXT		TXT	R	PXT
4		T	PXR		
5		R	PXT		
6	PXR		TXR		PXR
7	-48VDC	(-48VDC)	(-48VDC)		
8	GRD	GRD	GRD		
circuit pack	4-wire digital (8 ports)	2-wire digital (16 or 24 ports)	4-wire BRI Trunk Side	Analog line (16 or 24 ports)	Data Line

PX	PBX transmit	T	Tip	(A)
TX	Terminal transmit	R	Ring	(B)

Install the BRI terminating resistor

The resistors balance the cable plant between the receiver and the transmitter on the interface. When using the TN2198 ISDN-BRI 2-Wire U Interface circuit pack, use an NT1.

A terminating resistor is always required near the terminal when the BRI S-type interface circuit pack (TN556 BRI 4-Wire S-NT Line circuit pack) is used (see *#5ESS Switch Integrated Services Digital Network Customer Premises Planning Guide*, 533-700-100). The resistor is built into the NT1 and can be 1 of 3 values, depending on the configuration and the distance from the NT1 to the ISDN terminal. The NT1 controls the resistor's value; if needed, place a terminating-resistor adapter near the terminal and in the satellite closet or work location.

DANGER:

The 440A4 terminating resistor and 110RA1-12 terminating-resistor block are UL-listed. Most new installations are the 110RA1-12 terminating-resistor block. Observe the following installation instructions:

- *Never install telephone wiring during a lightning storm.*
- *Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.*
- *Never touch uninsulated wires or terminals unless the telephone line has been disconnected at the network interface.*
- *Use caution when installing or modifying telephone lines.*

Terminating-resistor adapter

Figure 34, 8-wide terminating-resistor adapter (440A4), on page 116 shows an 8-pin 440A4 terminating-resistor adapter. The adapter has an 8-wide plug at 1 end, a short cord, and an 8-wide jack at the opposite end.

Figure 34: 8-wide terminating-resistor adapter (440A4)

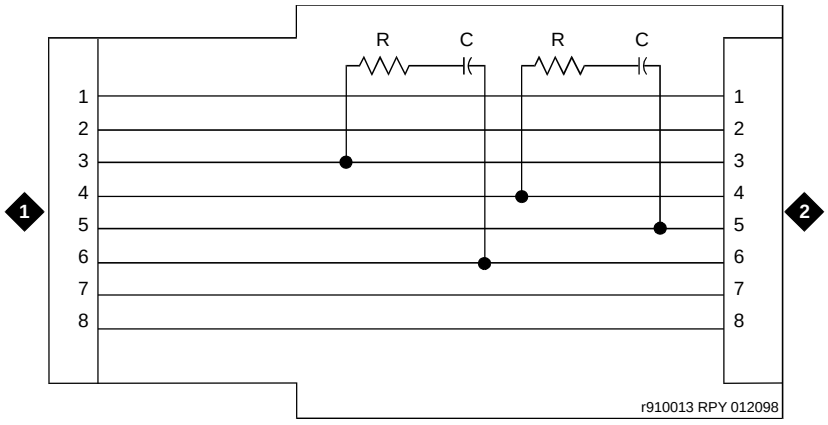


Figure notes

1 8-wide plug

2 8-wide jack

Closet-mounted (110RA1-12)

The 110RA1-12 terminating-resistor block consists of 12 2-pair circuits and provides the 100-Ohm termination used for ISDN-BRI circuits.

Figure 35, Terminating-resistor block (110RA1-12), on page 117 shows the wiring of the 110RA1-12. Three rows of 110D 4-connector blocks contain resistors and capacitors. The bottom row is designated as the input row and the top and middle rows are designated as the output rows. The circuit assembly is mounted on a standard 110A, 100-pair mounting base.

Figure 35: Terminating-resistor block (110RA1-12)

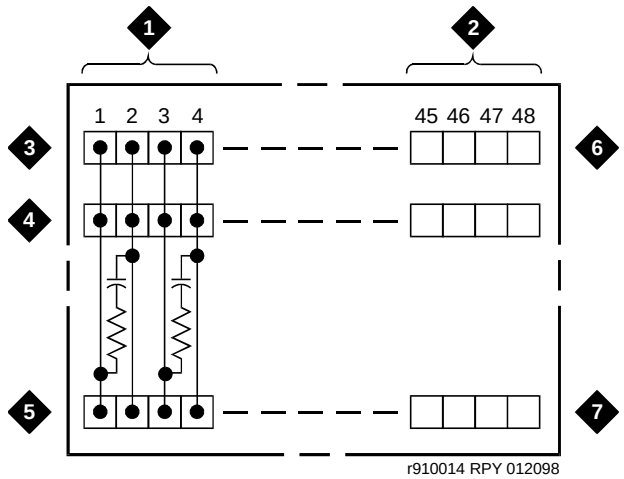


Figure notes

1	Circuit 1	**5**	Input row “C”
2	Circuit 12	**6**	Only 1st circuit shown to all 12 circuits (2APR) per block
3	Output row “A”	**7**	110D 4-connector block
4	Output row “B”		

Figure 36, Typical installation of terminating-resistor block, on page 118 shows the wiring connections for the 110RA1-12 terminal block. The TN556 BRI switch port is terminated to bottom row C.

Figure 36: Typical installation of terminating-resistor block

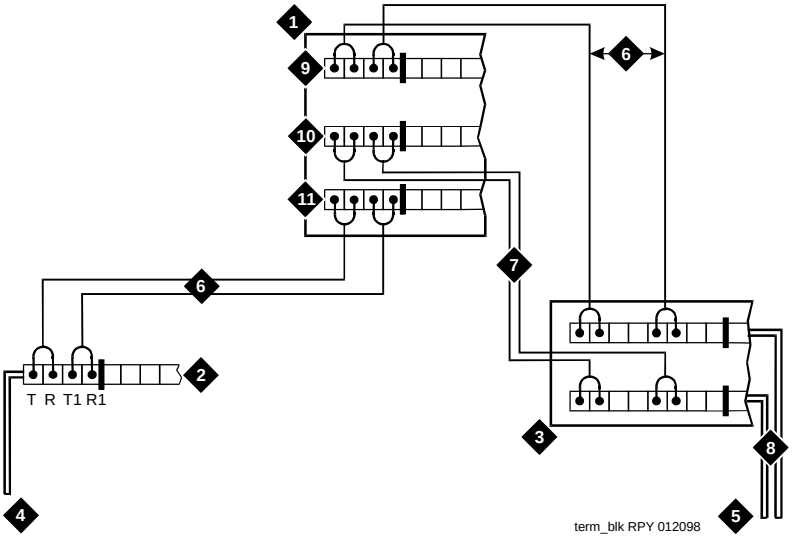


Figure notes

1	Part of terminating-resistor block	**7**	Basic multipoint option
2	White or purple field	**8**	4-pair horizontal cables
3	Part of 4-pair blue field	**9**	Row “A”
4	From ISDN T-interface circuit (2-pair)	**10**	Row “B”
5	To ISDN S/T-interface terminals	**11**	Row “C”
6	2-pair cross-connect		

For point-to-point wiring, the top row connects to the blue station field. The pair connects from the 110RA1-12 to the standard 4-pair circuit. Pair 1 from the 110RA1-12 connects to Pair 1 of the station field, and Pair 2 connects to Pair 3 of the station field.

Connect row B (output) to the 2nd terminal common to the multipoint circuit to accommodate basic 2-terminal multipoint applications.

Install multipoint adapters

Use multipoint adapters to provide signal fanout of the T-interface. BR851-B or the 367A perform fanout at the workstation. These adapters support more than 1 ISDN terminal per horizontal 4-pair D-inside wire (DIW). To support multiple horizontal runs, a MDF with multiple common rows performs fanout in the satellite closet. The 110RA1-12 provides fanout for 2 horizontal runs and contains the 100-Ohm terminating resistor. Use this for basic multipoint or point-to-point with terminating resistor in the closet. Other fanout blocks include the 110AB1-025M and the 110AB1-050M.

BR851-B adapter (T-adapter)

The BR851-B supports 2 terminals on 1 multipoint BRI at the workstation and is used to fanout transmission and power. See Figure 37, Wiring diagram of BR851-B, on page 119.

Figure 37: Wiring diagram of BR851-B

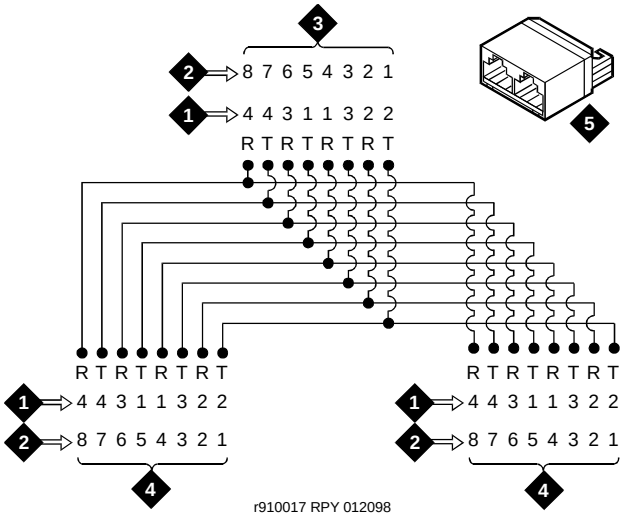


Figure notes

1	Wire pairs	**4**	Female
2	Pin numbers	**5**	T-type adapter (BR851-B)
3	Modular plug (male)		

367A adapter

The 367A adapter provides fanout for up to 7 terminals. See Figure 38, Wiring diagram of 367A adapter, on page 120.

Figure 38: Wiring diagram of 367A adapter

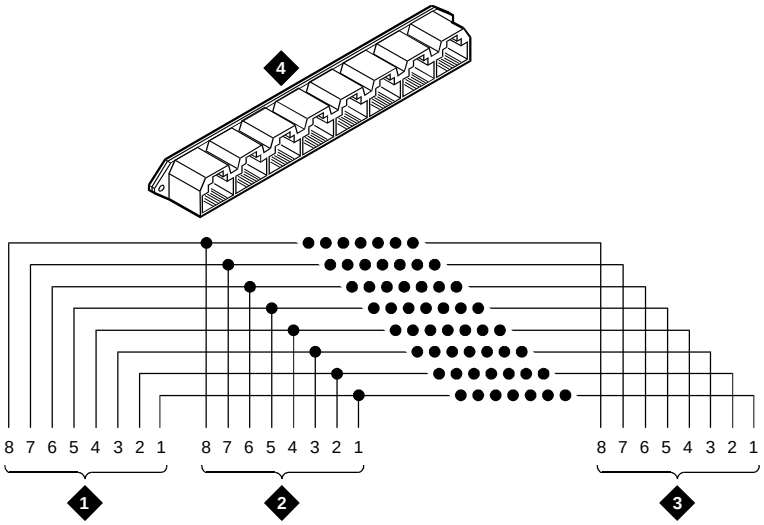


Figure notes

1	Jack 1	**3**	Jack 8
2	Jack 2	**4**	367A adapter

Basic multipoint installation distances

Figure 39, Basic multipoint with one work location, on page 121 provides cabling information for fanout of ISDN-BRI multipoint installations. The terminating resistor is located in the satellite closet. Every distance assumes 24-AWG [0.26-mm^2 D-inside wire (DIW)].

Figure 39: Basic multipoint with one work location

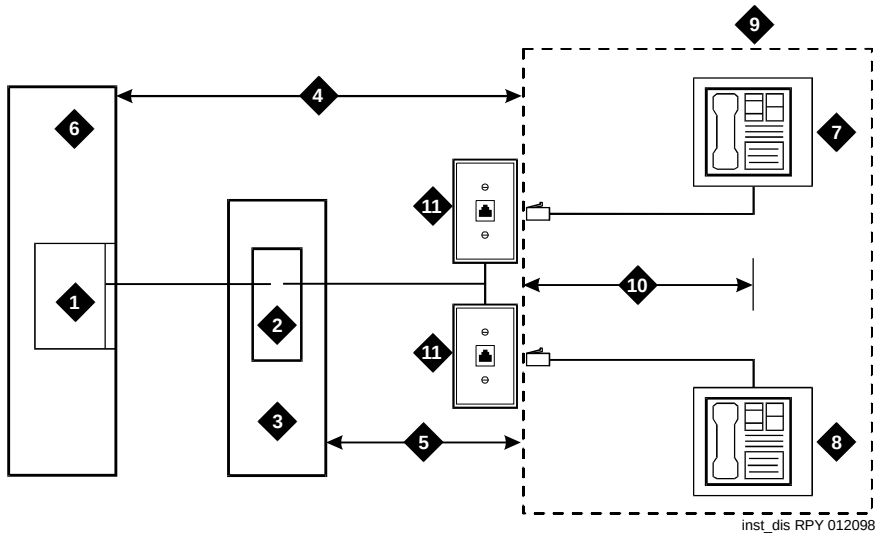


Figure notes

1	S-interface source (TN556)	**6**	System's cabinet
2	Terminating resistor	**7**	Terminating endpoint 1
3	Satellite closet	**8**	Terminating endpoint 2
4	Maximum distance from S-interface source to work location – 1600 feet (488 m)	**9**	Work location
		10	Maximum distance from information outlet to terminating endpoint – 33 feet (10 m)
5	Maximum distance from satellite closet to work location – 250 feet (76 m)	**11**	Information outlet

Install off-premises station wiring

The local telephone company provides the cabling for off-premises stations. These stations can appear on any of the RJ21X network interfaces provided for the CO trunks.

WARNING:

Use only an FCC-approved (or equivalent) analog telephone (for example, 2500-series set) as an off-premises station. The TN746B and TN2183 Analog Line circuit packs can be connected to off-premises stations.

1. Install an A25D cable between the RJ21X network interface and a sneak fuse panel.
2. At the MDF, connect jumper wires between 1 row/connecting block in the green field and up to 3 rows/connecting blocks in the purple field to concentrate the analog line pairs.
3. Connect an A25D cable between the sneak fuse panel and the terminal block connector associated with the green row in Step 2.
4. Install a green label on the terminal block to identify the remote location.
5. Administer per *Administrator's Guide for Avaya Communication Manager* (555-233-506).

Install off-premises or out-of-building stations

Out-of-building campus stations are telephones not physically located in the same building as the equipment room yet located on the same property.

Analog off-premises stations

Figure 40, Connections for one to eight out-of-building analog telephones, on page 123 shows the connections for 1 to 8 off-premises analog telephones. Only analog telephones connected to TN742, TN746B, TN2183, or TN769 Analog Line circuit packs can be installed out-of-building.

The maximum distance from the system's cabinet to the out-of-building voice terminal is 6000 feet (1828.8 meters) using 24-AWG (0.26-mm^2) wire.

Figure 40: Connections for one to eight out-of-building analog telephones

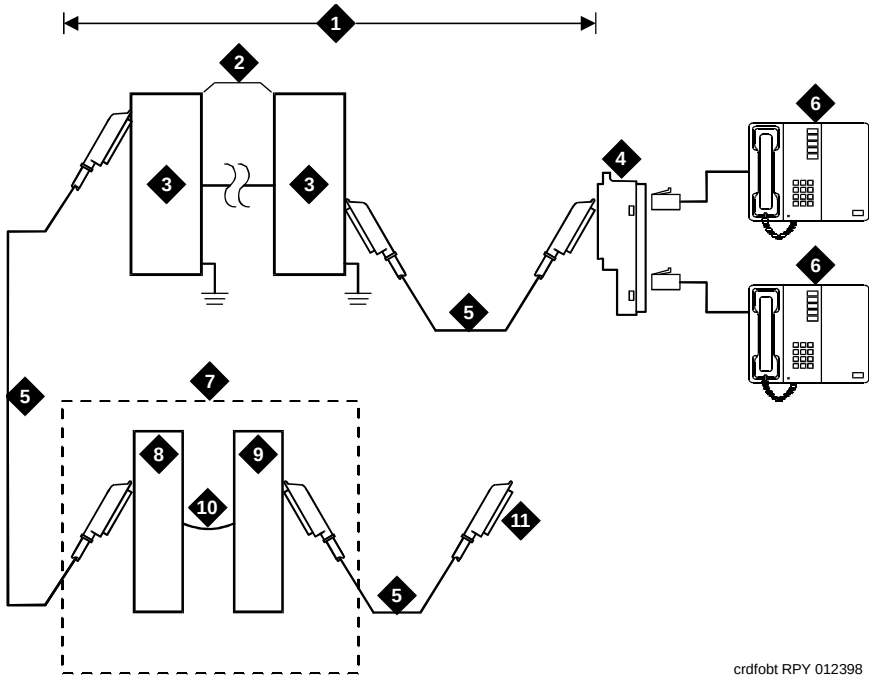


Figure notes

1	Locally engineered cables	**6**	Out-of-building analog telephones
2	Out-of-building wiring	**7**	Part of MDF or patch panel
3	Multipair protector units (primary protectors with heat coils or equivalent with sneak-current protection)	**8**	Station side (white field)
		9	System side (purple field)
4	356A adapter	**10**	Cross-connect jumpers
5	B25A cable	**11**	To Analog Line circuit pack (TN2183, TN769, TN742, or TN746B)

Figure 41, Connections to 24 out-of-building telephones, on page 124 shows the connections for up to 24 off-premises analog telephones, with concentrations of analog line pairs used at both buildings to minimize the off-premises wiring required. At the MDF, jumpers must be connected between 1 row/connecting block in the white field and up to 3 rows/connecting blocks in the purple field. At the station location, a WP-90929, List 1 concentrator cable is used. There are 8 station appearances on each of the 3 fingers of the concentrator cable. See Figure 41, Connections to 24 out-of-building telephones, on page 124.

Figure 41: Connections to 24 out-of-building telephones

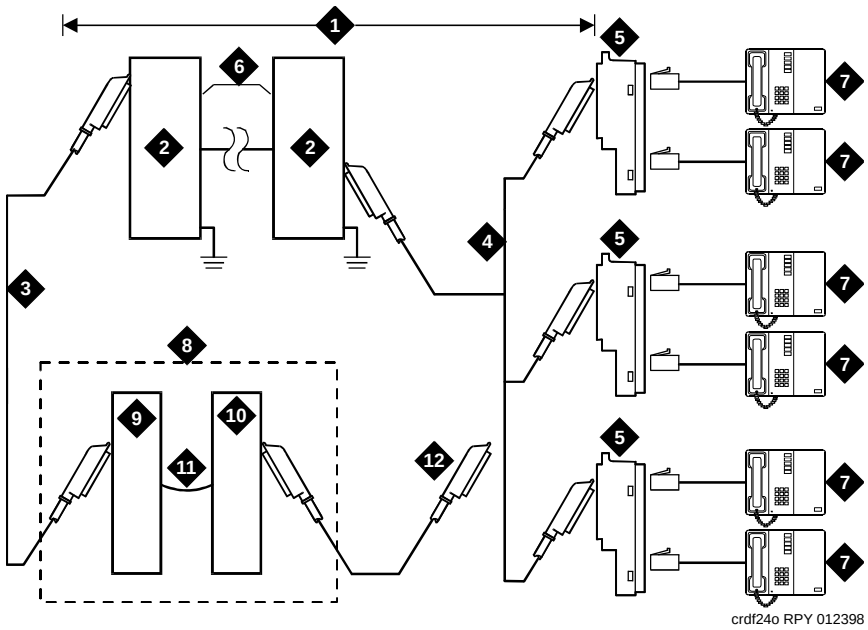


Figure notes

1 Locally engineered cables

2 Multipair protector units (primary protectors with heat coils or equivalent with sneak-current protection)

3 B25A cable

4 Concentrator cable (WP90929 List 1)

5 356A adapter

6 Out-of-building wiring

7 Out-of-building analog telephones

8 Part of MDF or patch panel

9 Station side (white field)

10 System side (purple field)

11 Cross-connect jumpers

12 To TN2183, TN769, TN742, or TN746B Analog Line circuit pack

Circuit protectors

Both building entrances require carbon block or equivalent protection and sneak-current protection. Provide this protection with a 4-type protector. The 4-type protector is equipped with a heat coil or a 3-type protector plus a separate sneak-current protector.

The 4-type protector is the preferred device. For installations not using primary protection, always use 4-type protectors. When the 3-type protector is already installed, a separate sneak-current protector is required. The multipair protector units and the off-premises cabling must be locally engineered. Connectorized multipair protector units (female 25-pair connector) are recommended.
Table 18, Analog line circuit protectors, on page 125 shows the recommended protectors.

Table 18: Analog line circuit protectors

Primary[1]	Primary (with heat coil)	Sneak-current protectors[1]
3B1A (carbon)	4B1C (carbon)	220029 Fuse
3B1E-W (wide-gap gas tube)	4B1E-W (wide-gap gas tube)	SCP-1
3C1S (solid state)	4C1S (solid state)	

1 The 3-type protectors should only be used if they are already part of the existing protection system. A sneak-current protector is always required when a 3-type primary protector is used.

An analog out-of-building (500-, 2500-, or 7100-series) telephone connected to an Analog Line circuit pack should be near enough that its maximum loop resistance does not exceed 1300 Ohms.

The following voice terminals *cannot* be installed in an exposed environment:

- 7300-series voice terminals connected to TN762 Hybrid Line circuit packs
- Multibutton Electronic Telephone (MET) sets connected to TN735 MET Line circuit packs
- Analog telephones connected to TN746 Analog Line circuit packs

See Table 3, Comcodes for equipment used with G600, on page 63 for circuit protector ordering information (comcodes).

Digital out-of-building telephones

Use the following equipment to protect digital out-of-building voice terminals and Digital Line circuit packs at both building entrances:

- 4C3S-75 Enhanced Protector
- ITW Linx Enhanced Protector

These units provide primary and sneak-current protection. The 4C3S-75 is equipped with a heat coil for sneak-current protection while the ITW Linx is equipped with replaceable fuses for sneak-current protection.

Use the 4C3S-75 only with Vintage 14 or newer TN754 circuit packs. The 4C3S-75 can be used on any vintage of the TN754B circuit pack. The ITW Linx may be used on any vintage of the TN754 circuit pack. Table 19, Digital voice-circuit protectors, on page 126 lists the approved protectors.

NOTE:
The TN2181 (2-wire 16-port Digital Line circuit pack) may not be approved for some out-of-building uses. Contact your Avaya representative for more information.

Table 19: Digital voice-circuit protectors

Circuit pack	Enhanced primary protector (with sneak-current protection)
TN754B/any vintage	4C3S-75 or ITW Linx
TN2181	4C3S-75 or ITW Linx
TN2224B/any vintage	4C3S-75 or ITW Linx

When possible, every new and reused wiring installation should use blocks that accept the standard 5-pin plug-in 4C3S-75 protector. However, this may not be cost-effective in some cases; for these installations, the ITW Linx protector may be installed. For example, if screw-type carbon block protectors (or other comparable plug-incompatible types) are in place, it may be too costly to re-terminate the outside cable on a 5-pin mounting block for only a few out-of-building terminals.

The ITW Linx Enhanced Protector may be installed in series with existing primary protection. Note the 4C3S-75 protector cannot be installed in series with other types of primary protection, but must be installed as the only protection on the line entering the building. For the 4C3S-75 protector, various 25-, 50-, and 100-pair protector panels are equipped with 110-type connecting blocks and/or RJ21X connectors. The ITW Linx Enhanced Protector mounts directly on connecting blocks and requires a separate ground bar.

The maximum range for out-of-building digital voice terminals is:

- 3400 feet (1036 m) when using 24-AWG (0.26-mm^2) wire
- 2200 feet (670 m) when using 26-AWG (0.14-mm^2) wire

With the use of a data-link protector (an isolating transformer used to remove phantom power on the system side and re-introduce it on the terminal side), the range can extend to

- 5000 feet (1524 m) using 24-AWG (0.26-mm^2) wire
- 4000 feet (1219 m) using 26-AWG (0.14-mm^2) wire

When using a protector, the voice terminal must be locally powered by an external power supply or through the AC power cord provided with some of the 7400-series voice terminals. Install the protector on the equipment side of the protection in both buildings.

See Table 3, Comcodes for equipment used with G600, on page 63 for circuit protector and data-link protector comcodes.

Install emergency-transfer panel and associated telephones

NOTE:
Install only 1 emergency transfer power panel per system.

An 808A emergency-transfer panel (or equivalent), mounted next to the trunk/auxiliary field, enables emergency transfer. See Figure 42, 808A emergency-transfer panel, on page 128. Also see Table 16, Emergency transfer and auxiliary power, on page 115 for the pinout of the AUX (J1) connector. The transfer panel provides emergency trunk bypass or power-fail transfer for up to 5 incoming CO trunk loops to 5 selected station sets. The 808A equipment's Ringer Equivalency Number (REN) is 1.0 Amp.

Use analog telephones for emergency transfer. The 500- and 2500-series telephones can also be used as normal extensions. Emergency transfer capability may be provided on analog CO and Wide Area Telecommunications Service (WATS) trunks.

At the MDF, the unit is controlled by a connection to a yellow terminal row/connecting block in the trunk/auxiliary field. The unit is controlled by -48 VDC from the EM TRANS RELAY PWR terminals.

Install the emergency-transfer panel

To install an 808A emergency-transfer panel:

1. Install the transfer panel on any mounting frame in either a vertical or horizontal position. The housing has ears for screw-mounting and cutouts for snap-mounting the unit in an 89-type mounting bracket.

   NOTE:
   Install the panel so it can be accessed only by authorized personnel. The location must meet standard environmental considerations such as temperature and humidity.

2. Verify that dial tone is present at each trunk circuit.

Figure 42: 808A emergency-transfer panel

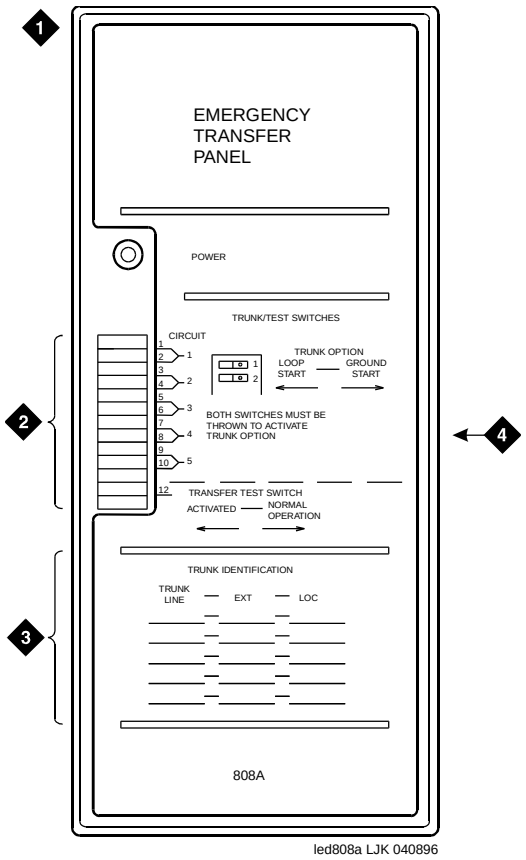


Figure notes

1	808A emergency-transfer panel	**3**	Trunk identification label
2	Circuit start selection switches	**4**	25-pair male connector

3 Locate the circuit start selection switches (the 1st 10 2-position switches on the left side of the 808A. See Figure 42, 808A emergency-transfer panel, on page 128.) These switches set each of the 5 incoming trunk lines to either loop start or ground start. Two switches are used for each of the 5 circuits; switches 1 and 2 are used for circuit 1, switches 3 and 4 are used for circuit 2, and so forth. See Table 20, Trunk/test switches, on page 129.

Table 20: Trunk/test switches

Switch number	Circuit number
1	1
2	1
3	2
4	2
5	3
6	3
7	4
8	4
9	5
10	5
11	Not used
12	Test switch

4 Connect a 25-pair cable between the male RJ21 25-pair connector on the 808A and the yellow field on the MDF. Table 21, Pin assignments for 25-pair connector on 808A, on page 130 shows the pinouts.

5 Make cross-connections for each emergency trunk/emergency station pair. See Figure 43, Connections for telephone used for emergency transfer, on page 132 and Figure 44, Connections for telephone used for emergency transfer and as normal extension, on page 133.

6 On the trunk identification label at the bottom of the panel, record the trunk line, extension, and location for each circuit.

7 To each voice terminal designated as an emergency terminal, attach a label identifying it as such. The labels are provided with the unit.

8 Check the system for normal operation as follows:

- **a** Place the test switch (switch 12) in NORMAL OPERATION.
- **b** Ensure the power supply is providing -48 VDC at 80 mA maximum. The power LED should be ON.
- **c** Check wiring connections.
- **d** Verify that there is dial tone on every emergency transfer set.

Table 21: Pin assignments for 25-pair connector on 808A ***1 of 2***

Pin	Color	Designation	Connector / Description
26	W-BL	TTC1	Tip-PBX Trunk Circuit 1
1	BL-W	RTC1	Ring-PBX Trunk Circuit 1
27	W-O	TTK1	Tip-CO Trunk Circuit 1
2	O-W	RTK1	Ring-CO Trunk Circuit 1
28	W-G	TLC1	Tip-PBX Line Port 1
3	G-W	RLC1	Ring-PBX Line Port 1
29	W-BR	TST1	Tip-Emergency Terminal 1
4	BR-W	RST1	Ring-Emergency Terminal 1
30	W-S	TTC2	Tip-PBX Trunk Circuit 2
5	S-W	RTC2	Ring-PBX Trunk Circuit 2
31	R-BL	TTK2	Tip-CO Trunk Circuit 2
6	BL-R	RTK2	Ring-CO Trunk Circuit 2
32	R-O	TLC2	Tip-PBX Line Port 2
7	O-R	RLC2	Ring-PBX Line Port 2
33	R-G	TST2	Tip-Emergency Terminal 2
8	G-R	RST2	Ring-Emergency Terminal 2
34	R-BR	TTC3	Tip-PBX Trunk Circuit 3
9	BR-R	RTC3	Ring-PBX Trunk Circuit 3
35	R-S	TTK3	Tip-CO Trunk Circuit 3
10	S-R	RTK3	Ring-CO Line Port 3
36	BK-BL	TLC3	Tip-PBX Line Port 3
11	BL-BK	RLC3	Ring-PBX Line Port 3
37	BK-O	TST3	Tip-Emergency Terminal 3
12	O-BK	RST3	Ring-Emergency Terminal 3
38	BK-G	TTC4	Tip-PBX Trunk Circuit 4
13	G-BK	RTC4	Ring-PBX Trunk Circuit 4
39	BK-BR	TTK4	Tip-CO Trunk Circuit 4
14	BR-BK	RTK4	Ring-CO Trunk Circuit 4
40	BK-S	TLC4	Tip-PBX Line Port 4

1 of 2

Table 21: Pin assignments for 25-pair connector on 808A ***2 of 2***

Pin	Color	Designation	Connector / Description
15	S-BK	RLC4	Ring-PBX Line Port 4
41	Y-BL	TST4	Tip-Emergency Terminal 4
16	BL-Y	RST4	Ring-Emergency Terminal 4
42	Y-O	TTC5	Tip-PBX Trunk Circuit 5
17	O-Y	RTC5	Ring-PBX Trunk Circuit 5
43	Y-G	TTK5	Tip-CO Trunk Circuit 5
18	G-Y	RTK5	Ring-CO Trunk Circuit 5
44	Y-BR	TLC5	Tip-PBX Line Port 5
19	BR-Y	RLC5	Ring-PBX Line Port 5
45	Y-S	TST5	Tip-Emergency Terminal 5
20	S-Y	RST5	Ring-Emergency Terminal 5
46	V-BL	COM1	Common 1 Relay Contact
21	BL-V	NO1	Normally Open 1 Contact
47	V-O	NC2	Normally Closed 2 Contact
22	O-V	NC1	Normally Closed 1 Contact
48	V-G	COM2	Common 2 Relay Contact
23	G-V	NO2	Normally Open 2 Contact
49	V-BR		
24	BR-V		
50	V-S	GRD	Ground From PBX
25	S-V	-48PX	-48V from Alarm Panel (AUX Cable)

2 of 2

9 Check the system for emergency transfer operation as follows:

- **a** Place the test switch (switch 12) in the ACTIVATED position.
- **b** Ensure that the power LED is off.
- **c** Verify there is CO dial tone for every emergency transfer set.

10 Connect the 808A to the MDF with a B25A or A25B cable. Figure 43, Connections for telephone used for emergency transfer, on page 132 shows the connections at the trunk/auxiliary field for a telephone used only for emergency transfer.

Figure 43: Connections for telephone used for emergency transfer

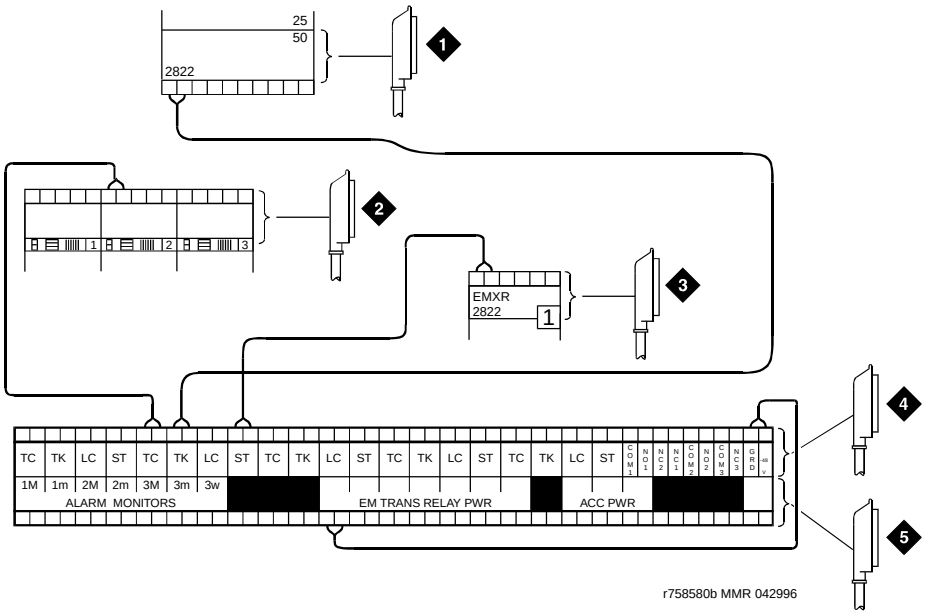


Figure notes

1 To network interface circuitry

2 To CO Trunk circuit pack

3 To blue or white station distribution field

4 To power-transfer unit

5 To control carrier's AUX connector

Figure 44, Connections for telephone used for emergency transfer and as normal extension, on page 133 shows the connections at the trunk/auxiliary field for a telephone used for emergency transfer and as a normal extension.

Figure 44: Connections for telephone used for emergency transfer and as normal extension

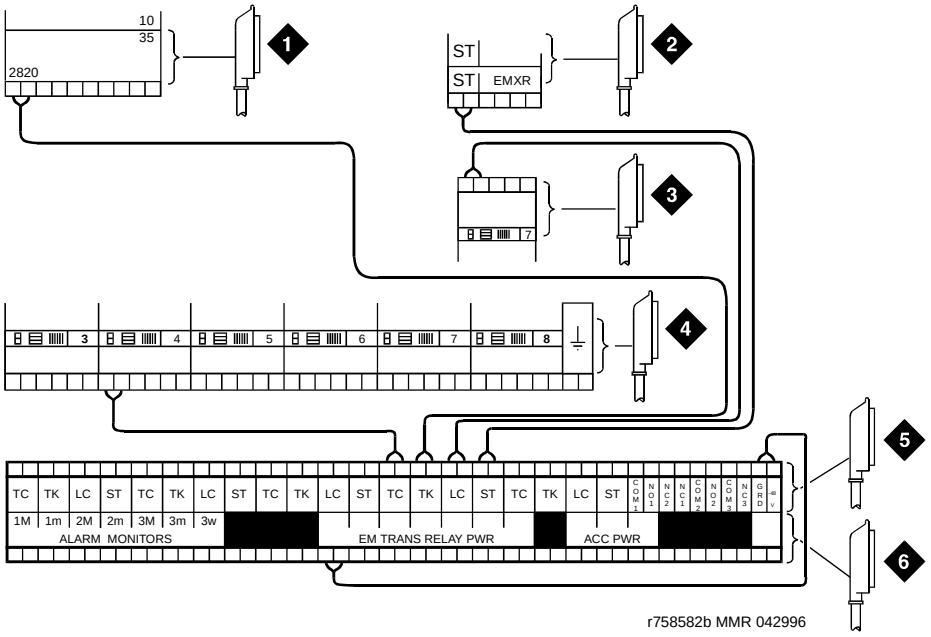


Figure notes

1	To network interface facility	**4**	To CO Trunk circuit pack
2	To blue or white station field	**5**	To power-transfer unit
3	To Analog Line circuit pack	**6**	To control carrier's AUX connector

Install telephone for power-transfer unit

Follow the appropriate procedure for your installation.

Trunk/auxiliary field: telephone used only for emergency transfer

1. Connect a pair of wires between the -48V and GRD terminals on the yellow emergency transfer row/connecting block and the EM TRANS RELAY PWR terminal. See Figure 43, Connections for telephone used for emergency transfer, on page 132.
2. Connect CO trunk leads from the purple field to the TC terminals on the yellow emergency transfer row/connecting block for each trunk.
3. Connect CO trunk leads from the green field to the TK terminals on the yellow emergency transfer row/connecting block for each trunk.
4. Connect the ST leads on the yellow emergency transfer row/connecting block for each emergency transfer telephone to the ST terminal appearance in the yellow trunk/auxiliary field. The ST terminal leads should be terminated on the following pairs: 1, 4, 7, 10, 13, 16, 19, or 22 (the 1st pair of any 3-pair group).
5. Connect the ST leads from the terminal in Step 4 to the assigned terminal in the blue or white station distribution field.

Trunk/auxiliary field: telephone used for emergency transfer and as normal extension

1. Connect a pair of wires between the -48V and GRD terminals on the yellow emergency transfer row/connecting block to the EM TRANS RELAY PWR terminal.
2. Connect CO trunk leads from the purple field to the TC terminals on the yellow emergency transfer row/connecting block for each trunk.
3. Connect CO trunk leads from the green field to the TK terminals on the yellow emergency transfer row/connecting block for each trunk.
4. Connect telephone leads from the purple analog line board row/ connecting block to the LC terminals on the yellow emergency transfer row/connecting block for each telephone.
5. Connect ST leads on the yellow emergency transfer row/connecting block for each emergency transfer telephone to the ST terminal appearance in the purple trunk/auxiliary field.
6. Connect the ST leads from the terminal in Step 5 to the assigned terminal in the blue or white station distribution field.

Telephone installation

1. Connect the telephone to the information outlet.
2. Install patch cords/jumper wires between the system side and the station side of the station distribution field on the MDF.

Connect modem to telephone network

1. Cross-connect the network jack on the modem to the network interface (via a 103A or modular wall jack). See Table 22, Pinout of network jack, on page 134 for the pinout.

Table 22: Pinout of network jack

Pin number	Signal
1	Unused
2	Tip
3	Ring
4	Unused

Figure 45: Network jack on US Robotics modem

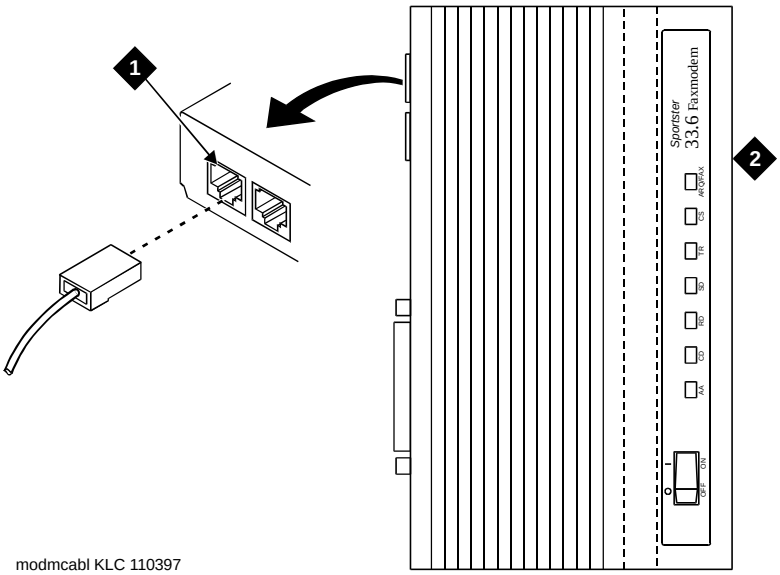


Figure notes

1 Pin 1 of network jack

2 Modem

Connect modem

The US Robotics external modem is the recommended external modem. A locally obtained, type-approved external modem may be used. Contact your Avaya representative for information.

If any other modem is installed, see the setup instructions provided with that modem.

Option settings for external modem

Use Table 23, Switch settings for US Robotics external modem,, on page 135 to check or set the 8 option switches on the US Robotics modem.

Table 23: Switch settings for US Robotics external modem, *1 of 2*

Switch	Setting	Function
1	OFF (up)	DTR (Data Terminal Ready) override
2	OFF (up)	Verbal result codes (text-formatted feedback characters such as *connected* or *no carrier*)
3	ON (down)	Enable result codes
4	OFF (up)	Displays keyboard commands (local echo)

1 of 2

Table 23: Switch settings for US Robotics external modem, *2 of 2*

Switch	Setting	Function
5	OFF (up)	Sets auto answer
6	OFF (up)	CD (Carrier Detect) override (modem sends CD signal on connect, drops CD on disconnect)
7	OFF (up)	Power-on and ATZ reset software defaults (loads Y or Y1 configuration from NVRAM)
8	ON (down)	AT (Attention) command set recognition (enables recognition, smart mode)

2 of 2

The modem is preconfigured to operate correctly. See Modem's configuration and administration on page 262 for procedures on how to verify that the correct defaults are set, how to configure the modem, and how to test the modem.

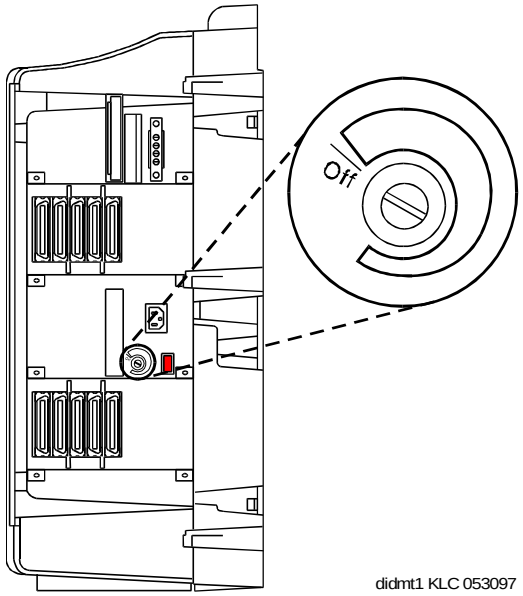
Set neon voltage to prevent ring ping

NOTE:
There is no need to set neon voltage on a G600.

NOTE:
If the ringing option is set to 50 Hz, neon voltage is not available. If 25 Hz is selected, the maximum voltage is 120 volts. See Set ringing option for CMC1 on page 385.

NOTE:
Set the control to **OFF** if there are no neon message waiting lamps or if LED message lamps are used. See Figure 46, Setting the neon voltage, on page 137.

Figure 46: Setting the neon voltage



1. Call a telephone with a neon message indicator and leave a message.
2. Check for ring ping (single ring pulse) each time the lamp flashes (approximately every 3 seconds).
3. Adjust the control clockwise in small increments until the ring ping stops. Ensure that the message lamp still lights when the adjustment is finished.

Complete installation

1. Disconnect the laptop.
2. Remove the RJ45 connector used to connect the laptop.
3. Insert the flash disk.
4. Set the left and right doors of the CMC1 onto the hinge pins and close the door(s). The doors must be closed to prevent EMI emissions. Tighten the door screws.
5. For the CMC1, set the right cover panel onto the right panel and secure. Do not use force.

View LEDs to determine power and fan alarm state

Use the LEDs on the front of each power unit to determine its state.

Table 24, LED and alarm conditions, on page 138 shows the LED and alarm conditions. Ring voltage and neon bus output do not activate alarm status.

Table 24: LED and alarm conditions

Condition	LED status	Alarm state	Fan alarm
Normal	Red off Yellow on	open	high
No input power	Red off Yellow off	closed	open
One or more DC outputs present	Red on Yellow off	closed	no state
Fan alarm	Red on Yellow off	closed	low

2 Connectivity and access to an S8100 system

To aid understanding of subsequent chapters, this chapter provides background information about connectivity and access to an S8100 system.

Physical connections and connectivity are as follows:

- Physical connections on page 139
  - Direct connection to the RJ45 service jack on page 140
  - Direct connection with a local monitor/ mouse/keyboard on page 149
  - Connection via customer's LAN on page 149
  - Connection via RAS (modem) dial up on page 149

The access method is determined by the task or access situation:

- Access methods on page 151
  - Via a Telnet session on page 152
  - Via a web browser session on page 153
  - Remotely using Avaya Site Administration on page 156
- Logins for the S8100 on page 158

This chapter begins with procedures for physically connecting to an S8100 with a G600 or CMC1. Once the physical connection is made to an S8100, you can access the system in any of several ways.

(See Appendix H, "Installation connectivity quick reference" for a tear-out "cheat sheet" summarizing physical connections, access methods, and login information.)

NOTE:
Detailed descriptions of the operation of the Microsoft Windows operating system and environments are beyond the scope of this document. Please refer to your Microsoft documentation for details concerning the Windows operating systems.

Physical connections

Use any of the following methods to create a physical connection to S8100 system:

- Direct connection via RJ45 jack on the TN2314 faceplate
- Direct connection via local monitor/mouse/keyboard
- Customer LAN
- RAS (modem) dial up
- DEFINITY LAN gateway (DLG)

Direct connection to the RJ45 service jack

Cabling to the RJ45 service jack on the S8100 server's (TN2314 circuit pack's) faceplate is the preferred method of connecting directly to an S8100 system.

Connect the laptop to S8100 system

The technician's laptop computer connects directly to the S8100 system. A media coupler cable is connected from the laptop's PCMCIA Ethernet card to a cross-over cable, which is connected to the RJ45 jack on the TN2314 circuit pack's faceplate. The laptop computer requires the following equipment:

Table 25: Technician's required laptop equipment

Part number	Description	Quantity
	Laptop computer running Windows 2000 or Windows 95 with a PCMCIA Ethernet card	1
	PCMCIA Ethernet card	1
848477634	Cable assembly to connect to RJ45: • Media coupler cable and/or RJ45 coupler (to connect the PCMCIA card to the cross-over cable). • RJ45 cross-over cable (approx.12 feet)	1

Figure 47: Laptop connection to the S8100 with the G600 or CMC1

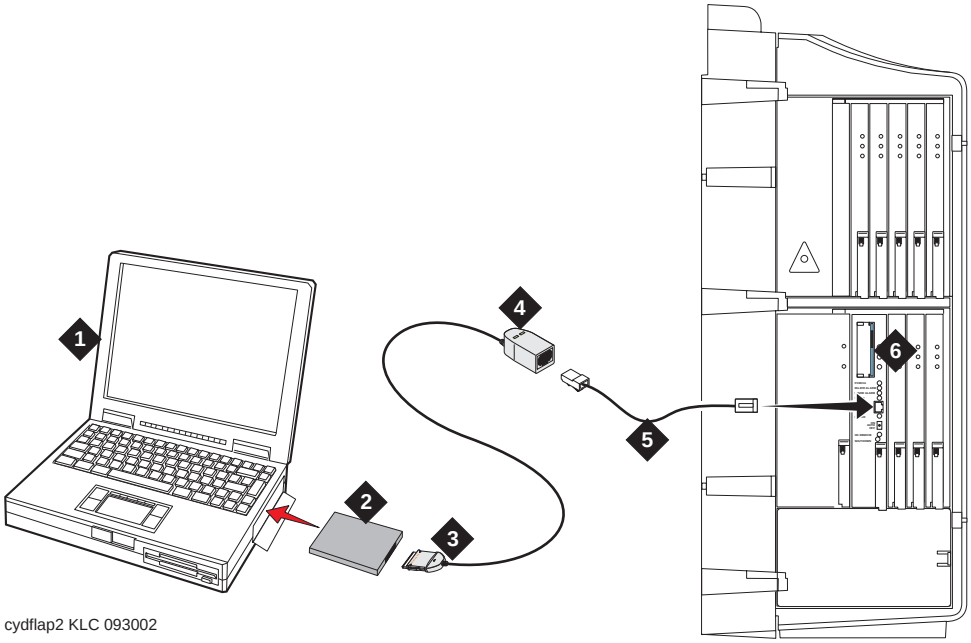


Figure notes

1	Laptop computer	**4**	RJ45 coupler (BRIA4P)
2	Laptop's PCMCIA Ethernet card	**5**	RJ45 cross-over cable
3	Media coupler	**6**	RJ45 jack

NOTE:
Figure 47, Laptop connection to the S8100 with the G600 or CMC1, on page 141 shows a CMC1 media gateway. For a G600 media gateway, the connection to the RJ45 jack on the TN2314 is the same.

Install the Ethernet card

1. Ensure the laptop's power is off.
2. Insert a PCMCIA Ethernet card into the laptop.

NOTE:
The Ethernet card can be any brand or model desired. A card with 100-Mbps capability provides faster response.

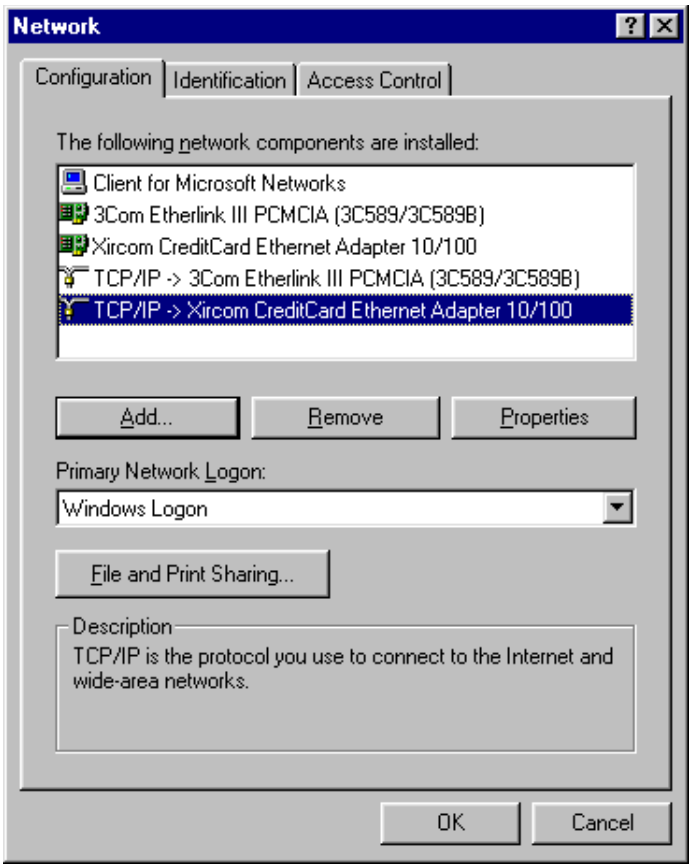
3. Using the RJ45 cross-over cable and the media coupler cable, connect the RJ45 jack in the TN2314 circuit pack to the laptop's Ethernet card. See Figure 47, Laptop connection to the S8100 with the G600 or CMC1, on page 141.
4. Power up the laptop and start Windows 95 or Windows 2000.

NOTE:
When changing computer settings in the following procedures, be sure to make note of ***and save*** both old and new information.

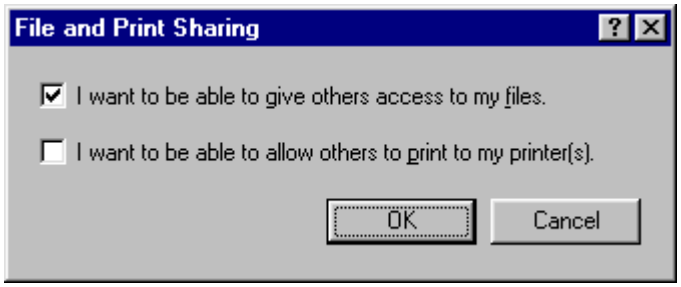
Configure the laptop (laptop running WINDOWS 95)

Set up the network PCMCIA interface to communicate with the S8100 system.

1. In Windows Explorer, right-click Network Neighborhood folder and click Properties.
2. In the Configuration tab, click File and Print Sharing.



The File and Print Sharing dialog displays:



3. Choose the I want to be able to give others access to my files box.
4. Click OK and return to the Network dialog.
5. Right-click Network Neighborhood and select Properties to return to the Network dialog.

6 Click the Access Control tab.

NOTE:
Before continuing, record the current settings on the Access Control tab. This information is needed to restore the laptop after work is finished with the S8100 system.

7 Ensure that Share Level Access Control is selected.

8 Click OK.

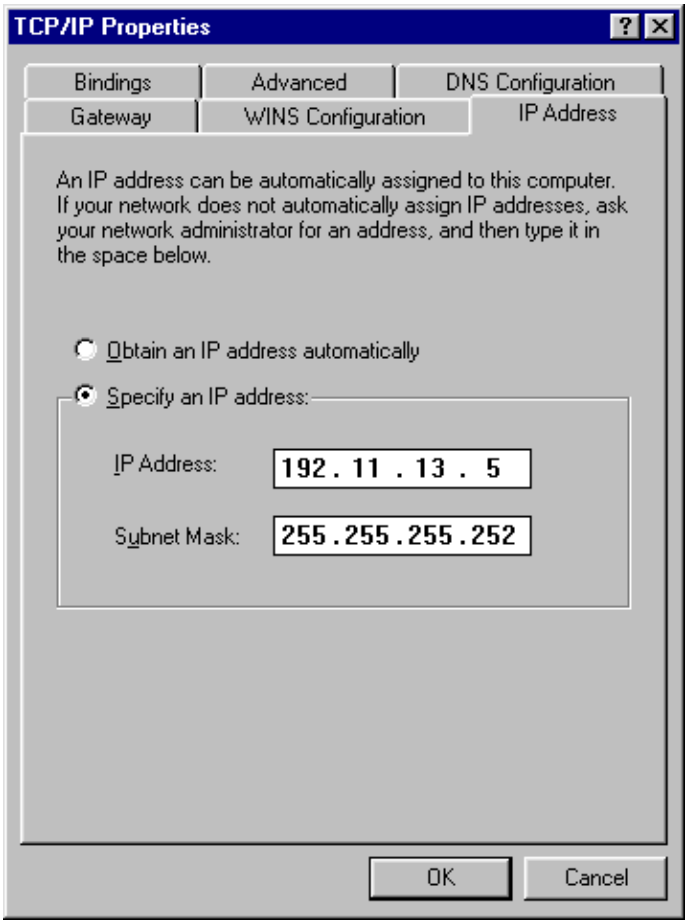
Click Yes if the following message displays: Do you want all connections to shared directories disabled? The connections are restored following a restart. Click No when asked whether to restart your computer now.

9 Right-click Network Neighborhood and select Properties to return to the Network dialog.

10 Select TCP/IP Xircom CreditCard Ethernet Adapter 10/100.

11 Click Properties.

The TCP/IP Properties dialog displays.



NOTE:
Before continuing, record the current settings from each of the TCP/IP Properties tabs. This information is needed to restore the laptop after work is finished with S8100 with a G600 or CMC1.

12 On the IP Address tab, ensure that Specify an IP address is selected. Type 192.11.13.5 as the IP Address and 255.255.255.252 as the Subnet Mask.

13 Click the DNS configuration tab. Click the Disable DNS radio button.

14 Click the WINS configuration tab. Click the Disable WINS Resolution radio button.

15 Click the Gateway tab. If a gateway is shown, record the gateway number. Highlight the gateway and select Remove.

16 Click OK here and in the following windows.

17 If asked, click Yes to restart your computer (or click Start → Shutdown → Restart the computer).

18 When the laptop reboots, verify that it is now connected to the S8100 system.

19 Start a DOS shell on the laptop by clicking Start → Programs → MS-DOS (for Windows 2000, click Start → Run → cmd).

20 In the DOS window type ping 192.11.13.6 and press Enter.

A series of 4 similar replies indicating successful response should display:

```
Reply from 192.11.13.6 bytes=32 time=1ms TTL=128
Reply from 192.11.13.6 bytes=32 time=1ms TTL=128
Reply from 192.11.13.6 bytes=32 time=1ms TTL=128
Reply from 192.11.13.6 bytes=32 time=1ms TTL=128
```

21 If a timeout reply displays, check cabling or review the previous setup steps. Also verify that the S8100 is operating normally and referencing the LEDs on the TN2314 circuit pack's faceplate. See Table 53, TN2314 circuit pack's LED states, on page 324.

Connect S8100 system to laptop's CD-ROM drive (laptop running WINDOWS 95)

To copy software from the laptop's CD-ROM drive to the S8100 server, you need to share the CD-ROM drive and establish a connection from the server to the drive.

1 On the laptop, double-click My Computer.

2 Right-click the CD-ROM drive icon and select Properties.

3 When the Properties dialog displays, click the Share tab.

4 Click Share As.

5 Enter a share name (for example, "Laptop CD").

6 Check the Full Access radio button.

7 Click OK to exit the windows.

The CD-ROM drive is now shared. The following procedures describe how to connect to the CD-ROM drive from an S8100 server.

1 Establish a connection from the laptop to the S8100 server.

   a On the laptop, open Internet Explorer and enter 192.11.13.6 (the IP address of the S8100 server) in the IE address window.

   b Click Administer System and login using lucent3 for the login ID and password.

   c Click the Continue button when the Notice screen appears.

   d Click Login to 192 under "Remote Control – Terminal Services."

   e If an error message appears, click OK.

f Click the Connect button (leave the Server: window blank).

g Click OK if an error message appears.

h Login using lucent3 for the login ID and password.

You should now be at the S8100 Windows desktop.

2 Connect back to the laptop's CD-ROM drive.

a On the S8100's desktop, click Start → Run and type in the path to the laptop's CD-ROM:

\\192.11.13.5\<***laptop's CD-ROM share name***>

where <laptop's CD-ROM share name> is the name you assigned to the laptop's CD-ROM drive when you shared it in the previous procedure (for example, "Laptop CD-ROM").

b You should now have access to the contents of the laptop's CD-ROM.

You can now copy files from the laptop's CD to the S8100 server's hard drive.

Restore the laptop's settings (laptop running WINDOWS 95)

When finished with an installation or upgrade, use this procedure to restore the settings on the technician's laptop to their original state.

1 Right-click Network Neighborhood. Select Properties.

The Network dialog displays.

2 Click the Configuration tab.

3 Click the File and Print Sharing button and select the I want to be able to give others access to my files box.

4 Choose Client for Microsoft Networks from the Primary Network Logon list.

5 Click the Identification tab and enter the computer name and workgroup.

6 Click the Access Control tab and check the appropriate boxes so that this dialog matches its earlier settings.

7 Click the Configuration tab.

- If a dialog appears notifying you that the security provider could not be found, click Yes.
- If the Authenticator type dialog appears, select Windows 2000 Domain, and click OK.

8 Double-click the modified component in the Network Components list. This should be the TCP/IP Xircom CreditCard Ethernet Adapter 10/100.

9 The TCP/IP Properties dialog displays.

10 Enter the original IP address and subnet mask.

11 Click the DNS Configuration tab to enable DNS. Enter the appropriate information.

12 Click the WINS Configuration tab to enable WINS. Enter the appropriate information.

13 Click the Gateway tab (if a gateway was used) and enter the appropriate information.

14 Click OK to close the TCP/IP dialog.

15 Click Yes to restart your computer.

When rebooted, the laptop returns to its original settings.

Configure the laptop (laptop running WINDOWS 2000)

Set up the network PCMCIA interface to communicate with the S8100 system.

1. In Windows Explorer, click Start → Settings → Network and Dial-up Connection → Local Areal Connection.
2. Click Properties.
3. In the list of components window, check “File and Printer Sharing for Microsoft Networks.”
4. Select “Internet Protocol (TCP/IP) and click Properties.
5. Check “Use the following IP address” radio button.

   NOTE:
   Before continuing, record the current settings from each of the TCP/IP Properties tabs. This information is needed to restore the laptop after work is finished with S8100 system.

6. Type 192.11.13.5 as the IP Address and 255.255.255.252 as the Subnet Mask. If Default Gateway has an IP address, record then remove it (or leave blank).
7. If there are DNS IP addresses in the Preferred and/or Alternate DNS windows, record them then remove them.
8. Click the Advanced button.
9. In the DNS and WINS tabs, record then remove any IP addresses.
10. Click OK here and in the following windows.
11. Start a DOS shell on the laptop by clicking Start → Programs → MS-DOS (for Windows 2000, click Start → Run → cmd).
12. In the DOS window type ping 192.11.13.6 and press Enter.

    A series of 4 similar replies indicating successful response should display:

    ```
    Reply from 192.11.13.6 bytes=32 time=1ms TTL=128
    Reply from 192.11.13.6 bytes=32 time=1ms TTL=128
    Reply from 192.11.13.6 bytes=32 time=1ms TTL=128
    Reply from 192.11.13.6 bytes=32 time=1ms TTL=128
    ```

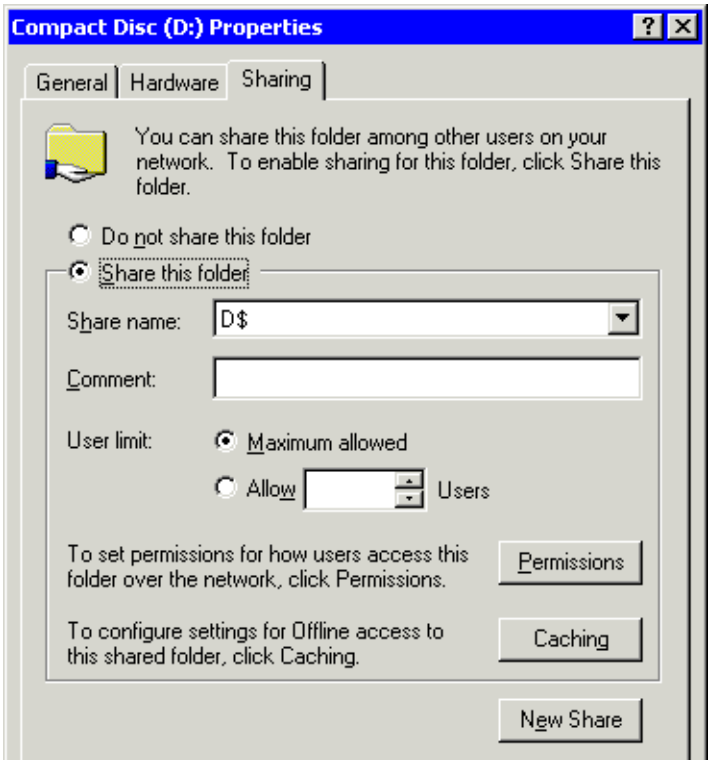
13. If a timeout reply displays, check cabling or review the previous setup steps. Also verify that the S8100 is operating normally and referencing the LEDs on the TN2314 circuit pack’s faceplate. See Table 53, TN2314 circuit pack’s LED states, on page 324.

Connect S8100 system to laptop’s CD-ROM drive (laptop running WINDOWS 2000)

To copy software from the laptop’s CD-ROM drive to the S8100 server, you need to share the CD drive and establish a connection from the server to the CD drive.

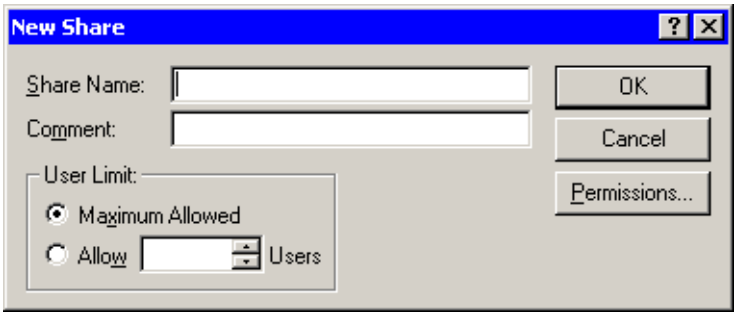
1. On the laptop, double-click My Computer.

2 Right-click the CD-ROM drive icon and select Sharing. The following dialog displays:



3 When the dialog displays, select Share this folder and click the New Share button.

The New Share dialog appears.



4 Enter a share name (for example, “Laptop CD-ROM”).

5 Select Maximum allowed for the User limit and click OK on the New Share and Properties windows.

The CD-ROM drive is now shared. The following procedures describe how to connect to the CD-ROM drive from S8100 server.

1 Establish a connection from the laptop to the S8100 server.

- **a** On the laptop, open Internet Explorer and enter 192.11.13.6 (the IP address of the S8100 server) in the IE address window.
- **b** Click Administer System and login using lucent3 for the login ID and password.
- **c** Click the Continue button when the Notice screen appears.

d Click Login to 192 under "Remote Control – Terminal Services."

e If an error message appears, click OK.

f Click the Connect button (leave the Server: window blank).

g Click OK if an error message appears.

h Login using lucent3 for the login ID and password.

You should now be at the S8100 Windows desktop.

2 Connect back to the laptop's CD-ROM drive.

a On the S8100 desktop, click Start → Run and type in the path to the laptop's CD-ROM:

\\192.11.13.5\<***laptop's CD-ROM share name***>

where <laptop's CD-ROM share name> is the name you assigned to the laptop's CD-ROM drive when you shared it in the previous procedure (for example, "Laptop CD-ROM").

b You should now have access to the contents of the laptop's CD-ROM.

You can now copy files from the laptop's CD to the S8100 server's hard drive or execute files on the laptop's CD from the S8100's desktop (for example, setup.exe).

Restore the laptop's settings (laptop running WINDOWS 2000)

When finished with an installation or upgrade, use this procedure to restore the settings on the technician's laptop to their original state.

1 Right-click Network Neighborhood. Select Properties.

The Network dialog displays.

2 Click the Configuration tab.

3 Click the File and Print Sharing button and select the I want to be able to give others access to my files box.

4 Choose Client for Microsoft Networks from the Primary Network Logon list.

5 Click the Identification tab and enter the computer name and workgroup.

6 Click the Access Control tab and check the appropriate boxes so that this dialog matches its earlier settings.

7 Click the Configuration tab.

- If a dialog appears notifying you that the security provider could not be found, click Yes.
- If the Authenticator type dialog appears, select Windows 2000 Domain, and click OK.

8 Double-click the modified component in the Network Components list. This should be the TCP/IP Xircom CreditCard Ethernet Adapter 10/100.

9 The TCP/IP Properties dialog displays.

10 Enter the original IP address and subnet mask.

11 Click the DNS Configuration tab to enable DNS. Enter the appropriate information.

12 Click the WINS Configuration tab to enable WINS. Enter the appropriate information.

13 Click the Gateway tab (if a gateway was used) and enter the appropriate information.

14 Click OK to close the TCP/IP dialog.

15 Click Yes to restart your computer.

When rebooted, the laptop returns to its original settings.

Direct connection with a local monitor/ mouse/keyboard

Use this method when plugging the monitor into an S8100 system, thus making it look like a PC. The Processor Interface cable is on slot 2 of the S8100 system. Customers have their own monitor/mouse/keyboard setup.

1 Plug the monitor into the Processor Interface cable behind the S8100 server (TN2314 Processor circuit pack).

2 Plug the mouse into the Processor Interface cable behind the S8100 server (TN2314 Processor circuit pack).

3 Plug the keyboard into the Processor Interface cable behind the S8100 server (TN2314 Processor circuit pack).

NOTE:
If these devices are plugged in while the system is running, you must reboot so that the system will recognize these peripherals. Once recognized by the system, the devices are hot pluggable.

Connection via customer's LAN

Customers may decide to connect the S8100 system to their LAN, which connects to the Ethernet jack of the Processor Interface cable. To configure the S8100 system as a node on the customer's network, see Set up customer's LAN parameters on page 163.

If the S8100 system is configured as a node on the customer's LAN, use a customer PC configured on the LAN to access it.

Connection via RAS (modem) dial up

NOTE:
This connection is not used for installations or upgrades.

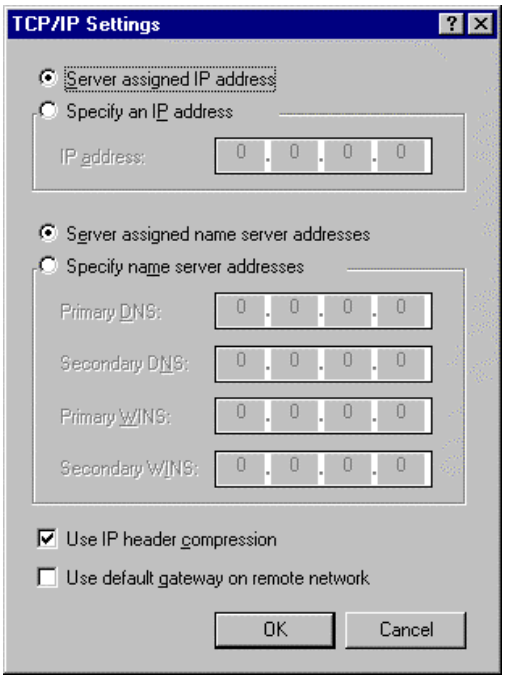
The RAS dial-up connection method enables Avaya services-related personnel, INADS, or customers to dial in remotely using a modem. On S8100 systems, the Windows 95 or Windows 2000 Remote Access Service (RAS) is listening for incoming calls from COM1, to which a modem is connected. Use the standard Windows 95 dial-up networking operation to set up this connection from a Services laptop computer as per the following procedure.

NOTE:
In Windows 2000, use the Make a New Connection wizard to complete this procedure. Just follow the on-screen instructions.

Create a connection icon

If a connection icon already exists, proceed directly to Click OK. on page 150. Otherwise, follow these steps:

1. Double-click Make New Connection on the Network Neighborhood Dialup Server Control Panel.
2. Enter the name of the computer you are dialing and select the appropriate modem.
3. Click Next.
4. Enter the area code and phone number of the system you are calling, then click Next.
5. Click Finish. The new icon appears in the Dial-Up Networking dialog.
6. Right-click the new icon to enable the associated properties window.
7. Click the Server Types tab of the associated properties window.
8. Select TCP/IP.
9. Click the TCP/IP Settings button. The TCP/IP Settings dialog displays:



10. Select Server assigned IP address.
11. Select Server assigned name server addresses.
12. Select Use IP header compression, and ensure that the Use default gateway on remote network is not checked.
13. Click OK.
14. The user name on this dialog must be “rasaccess” with the appropriate password. The password is the same for each S8100 system being contacted.
15. Click Connect.

16 A dialog similar to the following displays:

A network password is not needed unless disks will be mounted.

17 Leave the domain entry blank and click OK.

After a connection is established, a dialog similar to the following displays:

This indicates that the laptop is connected to the S8100 system. The dial-up connection is established.

Once the dial-up connection is established, the caller must use 1 of 3 access methods. See Access methods on page 151.

Access methods

Access the S8100 system through the following methods:

- Via a Telnet session on page 152
- Via a web browser session on page 153
- Remotely using Avaya Site Administration on page 156

Via a Telnet session

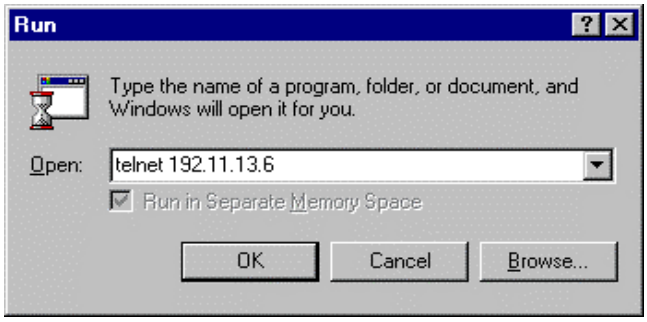
Use this access method to:

- Register S8100 system with INADS
- Activate license files
- Execute GAS commands from a bash shell
- Access S8100 system SAT session
- Set up the IP address for S8100 system using setip command

See Connect to SAT session via Telnet on page 296 for more information about connecting via Telnet.

NOTE:
The IP address differs depending on the type of physical connection established. See Appendix H, “Installation connectivity quick reference” .

1 On the laptop, click Start → Run from the Windows task bar. The Run dialog displays.

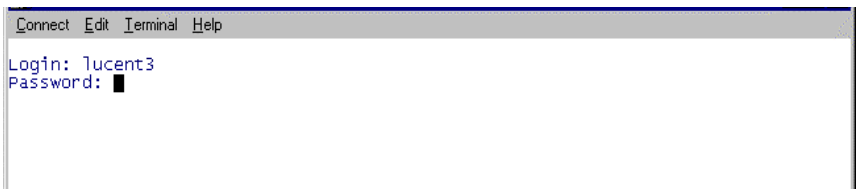


2 Enter telnet <***S8100 IP Address***>. If you are connected directly to the RJ45 service jack on the TN2314, use 192.11.13.6 for the IP address. If you are on the customer LAN, use the IP address of the S8100 server. Click OK.

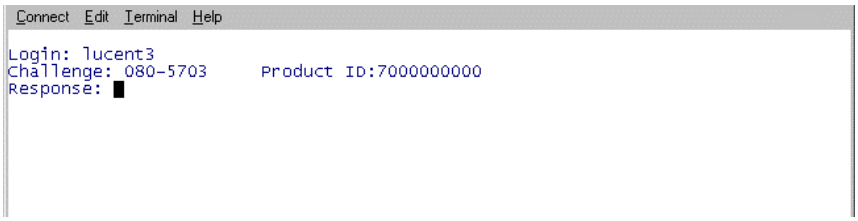
A Telnet session opens on your desktop.

NOTE:
There are 2 different scenarios, depending on whether the license file has already been installed.

a If no license file is installed, you are prompted for your login and password. The only valid login is lucent3. Enter lucent3 and continue to step 3.



b If the license file is installed, use any valid Lucent login. (See Logins for the S8100 on page 158 for a list of valid logins.) You will receive a challenge/response (instead of a password prompt) as shown in the following figures. Enter the response number and continue to step 3.



3 Once the Lucent Access Control (LAC) process accepts these inputs, it allows admission into the system.To continue, enter one of the listed commands (audix, bash, cmd, multivantage, help, exit) at the LAC prompt.

Via a web browser session

Customers or Avaya personnel use this method of access to the S8100 system (Windows 95 or Windows 2000 on their PC) to:

- Administer Communication Manager and INTUITY AUDIX (web access to Avaya Site Administration)
- Backup and restore
- Shut down the system
- Provide remote control using the Terminal Services client
- Download Avaya Site Administration and Message Manager.

  The software can be downloaded to the technician's laptop or a computer on the customer's network. The web browser provides a single point from which to start administration activity.

The web browser interface is available for use once a physical connection is established.

1 Open your web browser.

If your physical connection is a dial-up or an RJ45 direct connection, complete Step 2. If not, go to Step 3.

2 Verify that you are not using a proxy server:

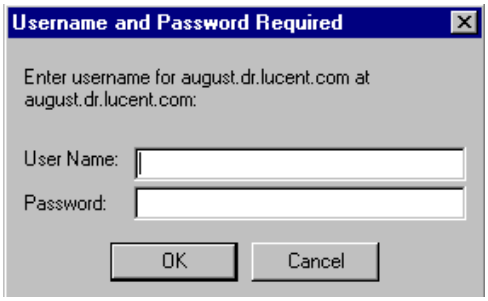
NOTE:
On Internet Explorer 5.x go to Tools, Internet Options, Connections; at the bottom of the window, click LAN settings; uncheck Use a proxy server box, and check Automatically detect settings; click OK until back to the web page.

3 Type http:// <ip address> in the address area of the web browser. The IP address also can be the name of the machine used. See Appendix H, “Installation connectivity quick reference” .

The S8100 home page displays:

4 Click Administer System.

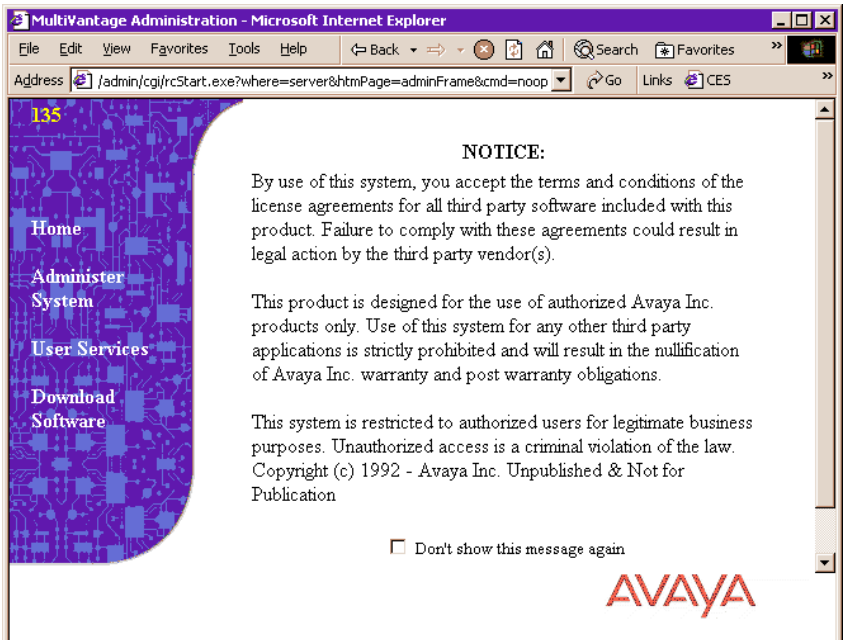
A dialog similar to the following displays:



5 Type lucent3 for both the user name and password.

6 Click OK.

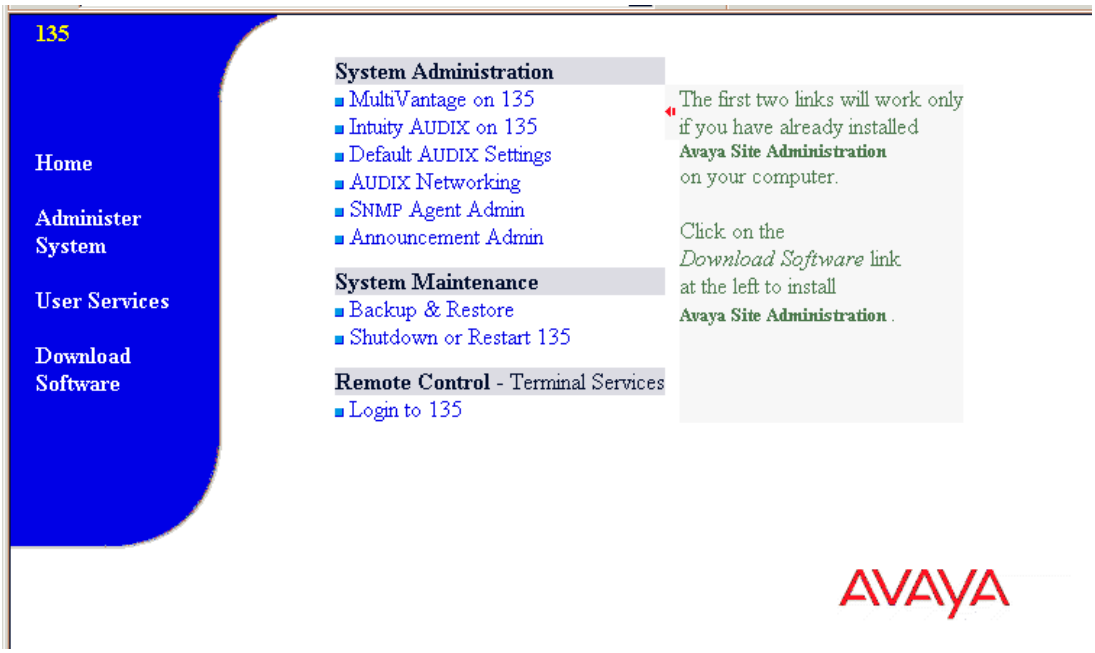
The following page displays:



7 Read the page and click Continue.

Once permissions are granted, the software allows you to navigate through the system.

8 Click “Administer System.” The Administration page displays:



Logging into the S8100 Windows 2000 desktop

1. On the Web Interface home page, click ‘Administer System’ and login using lucent3 for login and password. A domain is not required. Select 'continue' at license agreement window.
2. Click ‘Login to 192’ under Remote Control – Terminal Services.
3. If a VBScript error message appears, click OK.
4. Click the Connect button (leave the Server field blank).
5. If a VBScript message about fullsceen mode appears, click OK (you can resize the Terminal Services screen to full size by pressing ctlr-alt-Pause). A login window will open.
6. Login using lucent3. After login, the S8100 Windows 2000 desktop is displayed.

Remotely using Avaya Site Administration

If a customer wishes to dial in remotely using Avaya Site Administration, they must create a Windows 95 or Windows 2000 login with dialin permissions or give those permissions to an existing login. They should not receive the rasaccess login password, but they may receive the rasaccess IP address. They require the address to set up Avaya Site Administration or web-access connections to the system.

Dial-in permissions to an existing login

The system administrator can give dial-in permissions to an existing login by the following procedure:

1. Go to Start> Programs> Administrative Tools (Common).
2. Click User Manager.
3. Double-click an existing login that will be dialing in.
4. At the bottom of the ***User Properties*** window, click the Dialin icon.
5. Select the *Grant dialin permission to user* and *No Call Back* options, and click OK.
6. Click OK, and again in the ***User Properties*** window.
7. Exit User Manager.

Creating a login for remote access

The system administrator can create a login for remote access as follows:

1. Go to Start> Programs> Administrative Tools (Common).
2. Click User Manager.
3. On the top toolbar, click User, and select ***New User***.
4. In the dialog, assign the *Username* (this is the login) and the *Password*.

   NOTE:
   Full Name and Description are optional. The Options check boxes are the customer’s choice, but it is recommended that *User Cannot Change Password* and *Password Never Expires* should be the only ones checked.

5. Click Groups at the bottom of the dialog.

6 Make the login a member of *officeadmin* and *Users groups*, and click OK.

7 Click Dialin at the bottom of the dialog.

8 Check the *Grant dialin permissions* and *No Call Back* boxes, and click OK.

9 Click OK in the ***New User*** dialog.

10 Close User Manager.

Starting an Avaya Site Administration session

The customer must dial into the system to establish a PPP connection, and then start their Avaya Site Administration session. To set up a computer to dial into the system, perform these steps:

1 Go to My Computer.

2 Double-click Dial-Up Networking.

3 Double-click Make New Connection.

4 Fill in the *name* field; the system should fill in the correct *modem* attached to the PC; if not, choose the modem that is attached to the system.

5 Click Next.

6 Fill in the *Area code* and *Telephone number* for the system.

7 Click Next.

8 Click Finish in the window saying that the connection was created.

9 In the ***Dial-Up Networking*** window, right-click your connection icon.

10 Left-click Properties.

11 Click the ***Server Types*** tab.

12 In the ***Type of Dial-Up Server*** drop-down menu, select *PPP: Windows 2000, 95, NT 3.5, Internet*.

13 Under ***Allowed network protocols***, only *TCP/IP* should be checked.

14 Click OK, when finished.

15 Access the system by double-clicking the connection icon.

16 On the ***Connect*** screen, enter the correct *User name* and *Password*.

17 Click Connect.

18 When the connection is established, a screen appears. Click the Continue box.

NOTE:
A login window bay appear saying that the connection was successful.

Logins for the S8100

Avaya personnel logins

These are the S8100 logins for Avaya personnel. See Enable customer logins on page 173 for further information about logins.

Logins to enter the system	Logins to enter Communication Manager	Logins to enter INTUITY AUDIX
lucent1	dinit	atsc
lucent2	dinads	acraft
lucent3	dcraft	acraft

- Each row of logins has the same password. For example, the lucent1, dinit, and atsc logins all have the same password.
- The lucent logins are used for web browser, Windows 95 and Windows 2000 Terminal Server access.
- Every login works for Telnet access.
- The d... and a... logins (columns 2 and 3) are used for Avaya Site Administration access.

Avaya business partner and dealer logins

These are the S8100 logins for Avaya business partners and dealers. See Enable customer logins on page 173 for further information about logins.

Logins to enter the system	Logins to enter Communication Manager	Logins to enter INTUITY AUDIX
ntadmin This login is built into the system.	dadmin This login must be enabled in the license file.	sa This is the normal, customer-level, login on AUDIX – must be enabled manually.

3 System initialization

This chapter describes the procedures needed to initialize the S8100 system.

Starting with Release 10 for S8100, telephony features are activated or deactivated by the license file. The System Parameters Customer Options form is no longer used to activate/deactivate features – you can still display this form to see which features are activated, but you cannot use it to turn features on and off.

This chapter is organized as follows:

- Connectivity and access to the S8100 system on page 160
- Configure DHCP and TFTP servers on page 161
- Preliminary tasks on page 162
- License file, password file, and installation script overview on page 164
- Obtain the license and password files on page 165
- Obtain the installation script file on page 166
- Install the password file, license file, and installation scripts on page 168
- Resolve alarms on page 173
- Check system's status on page 173
- Place a test call on page 182
- Enable customer logins on page 173
- Administer S8100 on page 174
- Call accounting on page 185
- Administer Communication Manager for INTUITY AUDIX initialization on page 185
- INTUITY AUDIX administration on page 194
- Download Avaya Site Administration on page 197
- Administer SNMP on page 199
- Schedule backups on page 205

This chapter describes administration procedures using the SAT interface. Normally, this interface uses the function keys F1–F10 on your SAT terminal or PC to perform SAT functions. However, if you are running Windows 2000 on your PC and are using the W2KTT terminal emulation, you need to use Esc-key sequences to perform these functions instead of the function keys. The following table shows the escape-key sequence for each action.

Action	Esc Sequence
Help	Esc h
Cancel	Esc x
Submit	Esc e
Clear Field	Esc c
Prev Field	Esc f p
Next Field	Esc N
Previous Page	Esc p
Next Page	Esc n
Next Form	Esc f n
Go to Page	Esc d p
Edit vec	Esc f 6
Refresh	Esc r
Update Form	Esc u f
Logout	Esc l (lower-case L)

Connectivity and access to the S8100 system

The procedures in this chapter assume that you have followed the steps in Chapter 2, "Connectivity and access to an S8100 system" to:

- Connect a laptop to the S8100 system (or have established some other type of connection) as described in Physical connections on page 139.
- Set up the network parameters as described in Physical connections on page 139.
- Establish access to the S8100 system as described in Access methods on page 151.

Configure DHCP and TFTP servers

The S8100 system is shipped with DHCP and TFTP servers installed on the TN2314 Processor circuit pack. These servers can be used if the customer does not already have DHCP and/or TFTP servers on their network. To use the embedded DHCP and/or TFTP servers, they must be configured as described in this section.

DHCP server

IP addresses for IP telephones and other IP devices can be assigned manually. Alternatively, IP addresses can be assigned automatically using a DHCP server. Customers can use the DHCP server provided with the S8100 system or use a DHCP server already on their network.

CAUTION:
The S8100 DHCP server and another network DHCP server should not both be configured to support the same IP devices at the same time.

Enable the DHCP server

To enable the DHCP server on S8100:

1. From a Terminal Server session, click Start → Programs.

   If you receive error messages when starting a Terminal Server session, click **OK** for each error message.
2. Double-click Administrative Tools.
3. Double-click Services.
4. Double-click DHCP server.
5. From the Startup type drop-down menu, select Automatic.
6. If you want to start the server immediately, click Start.
   or
   If you do not want to start the server immediately, click OK and close every intermediate window.

   Servers that you selected a Startup Type of Automatic for will turn on every time you reboot the system.

For information about administering DHCP, see Chapter 4 in *4600 Series IP Telephone LAN Administrator's Guide*, 555-233-507.

TFTP server

A TFTP server is needed for downloading firmware to IP phones. Customers can use the TFTP server provided with the S8100 system or use a TFTP server already on their network.

Enable the TFTP server

To enable the TFTP server on S8100:

1. From a Terminal Server session, click Start → Programs.

   If you receive error messages when starting a Terminal Server session, click **OK** for each error message.
2. Double-click Administrative Tools.
3. Double-click Services.
4. Double-click TFTP server.
5. From the Startup type drop-down menu, select Automatic.
6. If you want to start the server immediately, click Start.
   or
   If you do not want to start the server immediately, click OK and close every intermediate window.

   Servers that you selected a Startup Type of Automatic for will turn on every time you reboot the system.

Preliminary tasks

This section lists the tasks needed to power up and check the software's version and serial number.

Power up and observe LEDs

When power is first applied to S8100, or when the system reboots, the LEDs on the TN2314 circuit pack light according to a predefined sequence. See LED boot sequence on page 321 for details about the power-up sequence.

Connect the laptop computer to S8100

For this procedure, see Connect the laptop to S8100 system on page 140.

Start a Telnet session

1. On the laptop, click **Start** → **Run** from the Windows task bar. The **Run** dialog displays.
2. Enter **telnet 192.11.13.6**. Click **OK.**

   A Telnet session opens on your desktop.
3. Enter **lucent3** for the login and password.
4. At the LAC prompt, type **bash**.

Verify the software's version number

The following procedure verifies the software's version number on the CD-ROM that shipped with the system.

1. From the BASH prompt, type **swversion** and press Enter. This displays information about the version of software running on the system. The first line displays a string like:

   Release=S8100-CM2.0-216.0

   which shows the software's load number (in this case, load 216).
2. Remove the CD-ROM that shipped with the system from the cabinet's door. Verify that the load number stamped on the CD-ROM matches the load number found in step 1.
3. If the load numbers match, determine the serial number. If not, the system's software may need to be updated before proceeding further.

Determine the serial number

1. From the BASH prompt, type **serialnumber** and press Enter.

   The serial number is read and displayed.
2. Ensure that the serial number matches the label on the front of the circuit pack. If it does not match, use the serial number you obtained from step 1.

NOTE:
The serial number obtained in step 1 is the firmware-embedded number and must be used.

NOTE:
The license file must contain a serial number that matches the serial number on your processor board. If it does not, you must obtain and install an new license file. For instructions on how to do this, go to http://www.avaya.com/services/rfa.

Set up customer's LAN parameters

This procedure administers the following customer-provided parameters:

- Computer Name ("Machine Name")
- IP address, subnet mask, and default gateway for the LAN connection via the Ethernet jack on the Processor Interface cable ("Splitter Cable")
- DNS IP addresses
- WINS IP address

CAUTION:
The S8100 is preconfigured to be a member of a local Workgroup and should not be made a member of a customer's Windows domain. If this is done, connectivity with Avaya Services will not operate correctly because user account authentication will no longer be done by the S8100. To check for proper workgroup membership, on the S8100 Windows desktop right-click the My Computer icon (this may have another name if the customer has changed it) and select Properties. Then choose the Network Identification tab to view the workgroup information.

From the BASH prompt, use the setip command to administer each parameter:

1. Type **setip name=<*machine name*>**
2. Type **setip cust=<*IP address, subnet mask, default gateway*>**
3. Type **setip dns=<*dns IP addresses and/or names*>**
4. Type **setip wins=<*WINS IP address*>**

   CAUTION:
   You must reboot the system for the machine name parameter to take effect. It is important to reboot at this point because subsequent procedures depend on the correct machine name.

5. Type **reboot nice.** The reboot process should take about 5 minutes.

See setip command on page 332, for more information about the **setip** command.

These parameters can also be set in the Network Places properties on the S8100 Windows 2000 desktop. In the event that customers require a new IP address, they can use the Terminal Services access to the S8100 Windows 2000 desktop.

License file, password file, and installation script overview

License file Remote Feature Activation (RFA) is a web-based application that enables the creation and deployment of license files for every switch. The license file enables the switch's software category, release, features, and capacities. License files are created using SAP order information and/or current customer configuration information. *Without a license file, the switch does not provide normal call processing.*

Without a valid license installed or a mismatched license:

1. The system generates a major alarm.
2. Depending upon the nature of the error, a 6-day countdown timer starts, but call processing continues unchanged.
3. If the countdown timer expires, the switch runs in Administration Mode only, and call-processing capability is limited to incoming and outgoing calls only to preadministered numbers.

   NOTE:
   Starting with Release 10, the *init* login cannot change the customer options, offer option, or special applications forms.

For customers with a maintenance contract, the installation script installs the following customer-related parameters: 1) RAS IP address, 2) product IDs (definity and audix), 3) alarm-destination number, and 4) alarm origination. The installation script file can be created and downloaded using the Automatic Registration tool (ART) on the ART web site.

For upgrades from pre-R10 software, the Feature Extraction tool must be run before the license file is created.

Using the Feature Extraction tool (for upgrades from pre-R10 only)

Use the Feature Extraction tool (FET) to capture (inventory) the customer options and other data from **pre-R10** DEFINITY server switches. You must do this before a valid license can be created.

FET produces an output file which is used by the Remote Feature Activation (RFA) to populate the system record with existing feature settings to support an upgrade to R10 or higher. This file containing existing switch configuration and the SAP order for the R10 or higher upgrade information together produces a valid license.

- If the switch has been upgraded to R10 or higher, do not use FET.
- Only a single FET output file can be imported for an individual system record.
- FET supports V4 to R9 DEFINITY server releases.
- Use the FET only when RFA cannot contact the switch remotely. Any customer may use this tool to capture their switch configuration and email the output file to the account team for the completion of a license.

The FET and instruction on how to use it are available at:
http://www.avaya.com/services/rfa.

Here is a summary of the steps to use FET:

1. Begin a transaction record in RFA.
2. Capture the transaction record.
3. Open and run FET.
4. Input transaction record #.
5. Store encrypted file produced by FET in local PC.
6. Go to RFA and complete your transaction record in order to create a license.

Obtain the license and password files

Perform the procedures in this section to obtain license and password files from the RFA web site.

RFA information requirements for new installations

1. Your personal Single Sign-On (SSO) for the RFA web site's authentication login.
2. SAP order number with RTUs
3. System ID
4. Module ID
5. Serial number of the TN2314 processor
6. Switch telephone number or IP address
7. Access to the RFA Information page for these items (if not already installed on your PC):

8. Adobe Acrobat Reader application installed on your PC (to read FET documentation)
9. Internet Explorer 5.0 or higher installed on your laptop/PC
10. Intranet access to your designated RFA portal (See the following URL list.)

Go to the RFA web site

The Remote Feature Activation (RFA) web site automates some of the installation procedures, including generating license and password files.

1. At your laptop/PC browser, go to the RFA web site:

   http://www.avaya.com/services/rfa
2. Using your SSO, log into the RFA web site.
3. Follow the links to the RFA Information page.
4. Complete the information necessary to create and deliver license and password files.

Obtain the installation script file

NOTE:
An installation script is needed only if the customer has a maintenance contract with Avaya.

You can download an installation script from the Automatic Registration tool's (ART's) web site.

Direct channels

For a direct channel (inside or outside the US), go to:

http://spiexp1.eng.avaya.com:8000/cgi-bin/ART/ARTstart.cgi

and follow these steps:

NOTE:
If you do not have a user ID and password for the ART database, select Administer my ART user ID and password and follow the instructions to create a new ID and password.

1. Select "Administer an S8x00 Server product for an install script".
2. Enter your ART user ID and password.
3. Record the ART session ID.
4. Enter the RFA System ID and the RFA Module ID, if applicable. If you do not have these ID numbers, enter the FL Number.
5. For Session Type, check the "Install Script for S8x00 Products".
6. For Product Type, select the "ECLIPS IP600".
7. Click the "Start IP Address Administration" button.

8 In the list of products table, click the product number (in the column labeled "**#**") corresponding to the product that you are creating the install script for. Typically, there is only one row in the table, and the product number is "**1**".

> **NOTE:**
> If the Product Alarm ID and/or RAS IP Address is listed as "N/A" in the table, these parameters are added automatically when the install script is created.

9 Check the following parameters and update if necessary:

- Communication Manager Release number
- Product (Nick) Name
- Alarm Origination set to **yes** – only if the customer has a maintenance contract with Avaya
- Dial-up destination number for alarm reporting (for example, INADS number)
- SRA IP address – only if SRA/SSG device is installed
- (Optional) INADS port number
- (Optional) SAP or DOSS order number

10 Click the "Continue Install Script for S8x00 Products" button.

11 Occasionally, the install script creation process will fail at this point due to network congestion and an error message appears. If this occurs, repeat steps 1–10.

12 A congratulations page appears when the install script is successfully created. Click the "Download" button.

13 Select "Save" to save the script file. Select the directory on your computer in which to save the installation script. You should save the script file with the default filename (which is typically "installscript.sh") unless there is a reason to change it (such as needing to distinguish between multiple script files).

Indirect channels

For an indirect channel (inside or outside the US), call your support organization for information about how to obtain an installation script file.

Install the password file, license file, and installation scripts

To install the license, password, and install script files, you must first copy them to the S8100 server's //d/LucentPub/ftproot directory.

Copy files to the server

To copy the license, password, and installation script files to the server, use FTP. Follow these steps:

1. Connect the PC/laptop to the RJ45 jack on the front panel.

   NOTE:
   For details of this procedure see Connect the laptop to S8100 system on page 140.

2. On the PC/laptop, click Start, Run, and type **telnet 192.11.13.6**; then click OK.
3. Login using lucent3 (default password is also lucent3).
4. Enter **bash** at the LAC prompt.
5. Enter **ftpserv** to start the FTP server.
6. Minimize the Telnet window.
7. Click Start, Run, and type **cmd** (or **command** for Windows 95) to open a DOS window.
8. Change directory to the storage location of the password, license, and install script files.

   (If these files are not in the same directory, move them so they are).
9. At the DOS prompt, enter **ftp -A 192.11.13.6**.

   This FTP command executes an anonymous login to the correct location for transferring the password and license files.
10. Enter **bin** to sets up the binary transfer type.

    "Type set to I" displays.
11. The installation script is used ***only if*** the customer has a maintenance agreement with Avaya.

    If so, enter **put <filename>** – where <filename> is the name of the installation script's file (for example, S8100D1installscript.sh) to transfer the installation script's file.
12. Enter **put password.bin** to transfer the password file from your laptop to the system.
13. Enter **put licensefile.lic** to transfer the license file from your laptop to the system.
14. Enter **bye** to close the FTP session.
15. Close the DOS window.
16. Maximize the Telnet window.
17. Enter **exit** to return to the LAC prompt.

Install the password, license, and installation-script file

As a result of the previous procedure, the license and authentication files (licensefile.lic and password.bin) should be in the //d/LucentPub/ftproot directory.

> **NOTE:**
> Business partners who login with a Windows administrator login, such as **ntadmin**, can execute the **loadpwd** and **loadlicense** commands from the bash shell.

1. Install the password file – At the LAC prompt, enter the command:

   loadpwd password.bin

2. Install the license file – At the LAC prompt, enter the command:

   loadlicense licensefile.lic

3. Enter **bash** at the LAC prompt.

4. Enter **cd //d/LucentPub/ftproot**.

   If using an installation script, install it by entering the following at the BASH prompt:

   S8100-lucent3> **./<*filename*>**

   where <*filename*> is the name of the installation script's file (for example, installscript.sh).

   > **NOTE:**
   > You need to use an installation script only if the customer has a maintenance contract with Avaya.

   This script assigns product ids, sets alarm origination and the alarm detection telephone numbers, and the RAS IP address. The system prompts you to reboot for the changes to take effect.

   If you were unable to successfully install the installation script in this step, you can set the customer-related parameters manually as described in the following section, Manually set S8100's customer-related information (alternative to ART) on page 170. Wait until after you have finished the manual procedure before rebooting. Also, if you are installing a license file, you should wait to reboot until after the license file is installed.

5. Installation of the password, license, and installation-script files is finished.

License file installation failure

The license file's installation will fail if:

- The processor's serial number in the license file does not match the serial number of the processor that is installed in the system.
- There is a software-version mismatch between the license file and the system.
- The license is expired.
- The license file is unreadable, cannot be decrypted, has the wrong length, has the wrong checksum, or has other format errors.

If the serial-number mismatch occurs because of a processor swap out, the serial number of the system's processor no longer matches the license file's serial number:

- Normal call processing continues.
- The system enters license-error mode.
- A major alarm is sent.
- The 6-day countdown timer starts. – Replace the old processor or install a new license file within 6 days.

Manually set S8100's customer-related information (alternative to ART)

The installation script downloaded from the ART web site normally configures every system parameter. Use the procedure in this section ***only if*** the customer has a maintenance contract ***and*** an installation script's file was ***not*** installed in the previous procedure, Install the password file, license file, and installation scripts on page 168.

NOTE:
Rebooting is required for these changes to take effect. To avoid multiple rebooting, set every customer-related parameter and license file installation before rebooting the system.

The customer-related parameters configured by this procedure are: 1) RAS IP address, 2) product ID (definity and audix), 3) alarm-destination number, and 4) alarm origination.

Manually setting RAS IP address:

To connect the system to the modem, you need to get the RAS IP address from the registration group at the time of License file generation. The recommended procedure is:

1. Telnet to the S8100 from the laptop.
2. Go to the "bash" shell from LAC by typing "bash".
3. Use the "setip" command to set the IP addresses. The format is:

   setip ras=<***RAS IP Address***> (for example, setip ras=198.152.30.15)

This completes the procedure to set the RAS IP addresses.

Instead of using the setip command, you could use the following alternative procedure:

Connect to the S8100 through the web interface. This is done by typing http://192.11.13.6 on the Internet Explorer with proxy server turned OFF. Login as "lucent3" and password "lucent3".

4. Go to the Administer system, which pops up the Screen to administer the system. Select the Terminal server option on the screen. (If you receive error messages when starting a Terminal Server session, click **OK** for each error message.) Login as "lucent3" and password "lucent3".
5. Select the Network Connections on the S8100 desktop and change the IP address on the incoming connections with the RAS IP address.

Manually setting product ID:

You need to set the product ID for each application. Get the product ID for each application from the registration group. The steps are:

1. Telnet to the S8100 from the laptop.
2. Go to the "bash" shell from LAC by typing "bash".
3. Use **productid** command to set the product ids on the S8100. There are two components – Communication Manager (MultiVantage) and AUDIX. Each component has a unique ID given by the services group at the time of registration.

   Use “productid multivantage-product-id 1xxxxxxxxx” to configure the Communication Manager ID.

   Use “productid audix-product-id 2xxxxxxxxx” to configure AUDIX ID.

Manually setting alarm origination and alarm-destination number

S8100 runs multiple applications on the platform. Every application reports problems to GAM (Global Alarming Module) which in turn calls out through the modem to the alarm-destination number. This is different from the INADS port on other Communication Manager servers, and needs to be configured using the "oss" bash command. The steps are as follows:

1. Telnet to S8100 from the laptop.
2. Go to the "bash" shell from LAC by typing "bash".
3. Use the “oss” command to set the alarm callout destination. The format is **oss 18005353573 3 3**. (The 1st parameter is the phone number of the alarm callout destination, the 2nd parameter is the number of retries, and the 3rd parameter is the retry count).
4. Type **alarmorig on** to turn on alarm origination.
5. Type **reboot immediate** to have the changes take effect.

   NOTE:
   Alarming will fail if Step 5 is not performed.

Administer no-license/emergency numbers

Without a valid license installed or a mismatched license:

1. The system generates a major alarm.
2. Depending upon the nature of the error, a countdown timer starts, but call processing continues unchanged.
3. If the countdown timer expires, the switch runs in Administration Mode only, and call-processing capability is limited to incoming and outgoing calls only to preadministered numbers.

To administer these numbers, follow these steps:

1. At the SAT type change system-parameters features and press RETURN. The Feature-Related System Parameters screen displays:

```
change system-parameters features           Page     4 of 12

                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM-WIDE PARAMETERS
                      Switch Name: Devo
     Emergency Numbers - Internal: XXXXXX External: XXXXXXXXXXXXXXXXXXXX
  No-License Incoming Call Number: XXXXX

MALICIOUS CALL TRACE PARAMETERS
               Apply MCT Warning Tone? n   MCT Voice Recorder Trunk Group:

SEND ALL CALLS OPTIONS
            Send All Calls Applies to: station
        Auto Inspect on Send All Calls? n

UNIVERSAL CALL ID
      Create Universal Call ID (UCID)? n      UCID Network Node ID:
```

2. Go to page 4. In the Emergency Numbers – Internal field (optional) type a valid extension (up to 5 digits).
3. In the Emergency Number – External field (required) type a 21-digit, dialpad-valid character string that can include trunk access codes. The default for this field is 911.
4. In the No-License Incoming Call Number field (optional) type a valid extension (up to 5 digits).
5. Press Enter to save the changes.

Alerts/notifications

A mismatched or missing license file generates these alarms or signals:

- Major alarm (LIC-ERR and NO-LIC) generated in the Hardware Error Log and Alarm Log (see Alarming strategy).
- Warning message at SAT login (see Log in warning messages).
- Lights an administered feature button (see Feature button assignments).

Test alarm call out

The following procedures are to be used to test alarming on S8100.

> **NOTE:**
> If testing remotely from the Technical Service Center (TSC), you must do the **rasdrop** command before doing any of the alarm tests. The **rasdrop** command forces a modem disconnect after 1 minute, and gives you time to execute the alarm test commands.

After each test has been run, the Field Services Organization (FSO) technician will have to go to the ART web site to verify each alarm has been received.

Communication Manager alarm test

1. Access the S8100 from the SAT.
2. At the command line, type **test inads**.
3. Press Enter.

INTUITY alarm test

1. Access the **bash** from the LAC.
2. At the prompt, type **logsend -tTST**.
3. Press Enter.

This will result in an INTUITY AUDIX alarm that should retire within a half hour.

Windows 2000 server alarm test

1. Access the **bash** from the LAC.
2. At the prompt, type **wrntevent GAM 0 9991**.
3. Press Enter.

NOTE:
This causes a Major GAM alarm. After the system has called out, enter **cleargamalarm all** at the **BASH prompt** to retire the alarm. This alarm also causes a Maestro case to be generated that will need to be closed by the INADS group.

Resolve alarms

To resolve any alarms. Refer to *Maintenance for Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways* (555-233-149).

Check system's status

See Avaya (Lucent) access controller bash commands on page 329 **for information about bash commands that are used in installation and administration.**

1. Open a LAC bash shell.
2. **To verify system health, execute d1stat and alarmstat.**

Enable customer logins

See Appendix B, "Set up customer logins" for information about setting up customer logins.

Enable INTUITY AUDIX logins

See Set up login accounts on page 290. Appendix B also includes information about the INTUITY AUDIX logins (sa, vm, and browse), the uses of each login, and the INTUITY AUDIX commands accessible to each login.

Enable customer's web logins

When the system leaves the factory, the only login that has access to the web interface is the login NTadmin. The customer may wish to create additional logins; for example, to download the Message manager. See Windows logins for customers on page 286.

Enable S8100 Logins

See Communication Manager logins for customers on page 291.

Administer S8100

This section describes the initial administration procedures.

S8100 commands

S8100 bash commands are useful for administration and installation tasks. These commands are allowed for the Avaya services login. See Avaya (Lucent) access controller bash commands on page 329, and *Maintenance for the Avaya S8100 with the Avaya G600 and CMC1 Media Gateways* (555-233-149) for information about these commands.

Set system date and time

The system date and time can be set using the S8100 Windows 2000 desktop to set daylight savings rules and the time zone as well as the date and time.

Alternatively, you can use the bash command, systime, to set the system time.

Using Windows 2000

Use Windows 2000 to set daylight savings rules and time zones, as well as the system date and time.

Use a laptop or a keyboard, mouse, and monitor, to login to the system.

Establish a terminal servers session through the web interface. On the Windows 2000 desktop, double-click the time icon in the tool tray at the lower right of the desktop. A window opens enabling you to set the date/time parameters.

Using systime

Avaya services logins can also use the command-line interface to set the date and time. Telnet to the LAC prompt, and enter the following bash command:

systime hh:mm (Use military time. For example, 16:00 represents 4:00 PM.)

Using a local command-line interface (CLI)

The date and time can also be set via the command-line interface similar to MS_DOS™. Only Avaya services logins can use this procedure. You will not be able to set the time zone or automatic daylight change with this method, but updating the time is possible. Perform a telnet to the LAC, and choose cmd. From a local keyboard, mouse, and monitor, perform the following:

1. Click Start, Run on the desktop.
2. In the window, type *telnet 192.11.13.6,* and click OK.
3. Login.
4. At the LAC prompt, type *cmd* and press Enter.
5. At the cmd prompt, type *date* and enter date (for example, *12/06/2001*); then press Enter.

   The system displays the date.
6. At the cmd prompt, type *time* and enter time using a 24-hour clock (for example, *13:45*); then press Enter.

   The system displays the time.

NOTE:
The technician can also do this from the laptop using the Service Access jack on the front of the TN2314 board, and following the same procedure.

Remote dial-in

If the customer needs to dial-in remotely, they will have had to set up the S8100 Media Server with dial-in permissions. If this has been done, perform the following steps:

1. On your PC, right-click My Network Places and select Properties.
2. Double-click **Make New Connection**.
3. Click **Next**.
4. Select the radio button “elect the radio button “Dialup to private network”
5. Click **Next**.
6. Type in the *Area code* and *Telephone number* for the system.
7. Click **Next**.
8. Select one of the radio buttons, “Create this connection for all users” or “Only for myself”
9. Click **Next**.
10. Type a name for the connection in the Name window
11. Click **Finish**.

12 In the Dial-Up Networking window, right-click your **connection icon**.

13 Click **Properties**.

14 Select the **Networking** tab.

15 In the *Type of Dial-Up Server* drop-down window, select **PPP: Windows 95/NT 4/200, Internet**.

16 Under *Allowed network protocols*, only **TCP/IP** should be checked.

17 Click **OK** when finished.

18 Access the system by double-clicking the connection icon.

19 On the connect screen, type in *User name* and *Password*.

20 Click **Connect**.

21 When the connection occurs, a screen opens. Click the **Continue** box.

22 A login window may appear, saying that the connection was successful. Click **OK**.

The dial-up connection drops down to the tray on the taskbar next to the Time.

23 Once the dial-up connection is established, return to step 1 of the previous section.

Set up country-specific call-progress tones

By default, the call-progress tones of the United States are used for each S8100 system. Using the mvdsp.sh shell script, you can change the system so that it recognizes the call-progress tones specific to your country.

The system gets it's translation of call-progress tones from a file named dsp0.USA. You can overwrite this file with one that contains translations that are appropriate for your country.

To set up country-specific call-progress tones:

1 Start a Telnet session.

For more information, see Start a Telnet session on page 162.

2 Go to a LAC prompt and execute a bash shell.

For more information, see Appendix G, "GAS commands in bash".

3 At the BASH prompt, enter **shutdown Audix**.

The bash shell is case-sensitive, so be sure to capitalize the first letter in Audix.

It will take a few minutes for AUDIX to shutdown, please be patient. A status message of "shutdownproc succeeded" displays when the shutdown finishes.

4 Enter **shutdown CornerStone**.

The bash shell is case-sensitive, so be sure to capitalize the C and S in CornerStone.

This process should finish very quickly. A status message of "shutdownproc succeeded" displays when the shutdown finishes.

5 Enter **d1stat**.

Confirm the following results:

CornerStone	PARTIALLY UP
Audix	DOWN
AudixNet	DOWN

If any of these 3 systems are still UP, repeat steps 3 to 5.

6 Enter: **cd //c/lucentsoftware/cornerstone/asp/dsp0**.

This moves you to the directory where the active tone detector file is, dsp0.USA.

7 Enter **pwd** to confirm you are in the correct directory.

The path of the current directory displays.

8 To verify the mvdsp.sh script is present, enter **ls**.

If you do not see the mvdsp.sh script, contact Tier-3 or -4 personnel for assistance.

9 Enter **. mvdsp.sh** to execute the mvdsp.sh script.

The following line displays:

Select dsp file [AUSTRALIA|BRAZIL|CANADA|MEXICO|UK|OTHER]:

NOTE:
You can exit from the script at any time by pressing **Ctrl C**.

10 In all-capital letters, enter one of the displayed countries or **OTHER**.

If you entered OTHER, you are prompted to enter the name of your country in all-capital letters. Make certain a tone detector file exists for your country and you enter it correctly.

NOTE:
If you enter in an unrecognized country, you are returned to the prompt to enter a valid country name.

Your country's translation file for call-processing tones is copied into "dsp0.USA". Meanwhile, the old "dsp0.USA" file is saved as "dsp0.USA.sav" in case you need to restore these settings.

You are successful when the "dsp file successfully copied" message displays. It is now safe to start CornerStone and AUDIX.

11 Use the log file to confirm successful completion.

12 Enter **start CornerStone**.

The message "addproc succeeded" displays upon successful completion.

This command will start AUDIX as well as CornerStone.

13 Enter **d1stat** to confirm that CornerStone and AUDIX are UP.

Call processing will now be based on the tones specific to your country.

Enable and disable SNMP

By default, SNMP is enabled on CMC1. If you are not using SNMP, disable it.

To disable SNMP, enter **d1disable snmp** from a bash session. The command **d1disable snmp** disables SNMP from being run when CMC1 is started.

To enable SNMP, enter **d1enable snmp** from a bash session. The command **d1enable snmp** enables snmp so that it automatically runs when CMC1 is started.

You must reboot your system for the SNMP settings to be effective.

Check customer option screen

From SAT, type **display system-parameters customer-options** and press Enter to display the system parameters customer options screen. Ensure that the version is V10.

The license file you downloaded from RFA and installed on the switch will activate RTU features on system parameters customer options screen. The “init” logon no longer controls access for activating an RTU (right to use).

Please check to ensure that the default and optional features and capacities on the screen coincide with the customer’s order. To check the relationship between what was ordered and what was populated on the screen, please go to the RFA information page see Go to the RFA web site on page 166. Go to the help information section of the RFA page, where you will find a material code/feature job aid that details the mapping between the material codes that RFA processes and the features, capacities, and release on the systems parameters options screen. If there is a problem with the customer’s order, please contact the account team so they can issue another order which will generate a corrected license file from RFA.

Set country options

To turn off the red alarm LEDs, some of the country options must be set on the Change System-Parameters Country-Options screen, shown in the following step.

1 Enter **change system-parameters country options**, and press **ENTER**.

A screen similar to the following displays:

```
change system-parameters country-options                    Page  1 of  23
                    SYSTEM PARAMETERS COUNTRY-OPTIONS
            Companding Mode: Mu-Law          Base Tone Generator Set: 1
       440Hz PBX-dial Tone? n              440Hz Secondary-dial Tone? n
     Analog Ringing Cadence: 1     Set Layer 1 timer T1 to 30 seconds? n
   Analog Line Transmission: 1
64/84xx Display Character Set: Roman
      Howler Tone After Busy? n   Disconnect on No Answer by Call Type? n
TONE DETECTION PARAMETERS
         Tone Detection Mode: 6
            Interdigit Pause: short
```

The default (United States) companding mode is **Mu-Law**. If the country uses A-Law companding, proceed to the next step.

2 Enter **A-Law** and click **Enter**.

NOTE:
Other items eventually need to be entered on this screen, but this is sufficient to turn the red alarm LEDs off.

The country codes are set as needed according to the following fields:

1 Digital Loss Plan

2 Analog Ringing Cadence

3 Analog Line Transmission

4 See Table 26, Country Codes, on page 179.

Table 26: Country Codes

Country	Code	Country	Code
USA	1	France	12
Australia	2	Germany	13
Japan	3	Czechoslovakia	14
Italy	4	Russia	15
The Netherlands	5	Argentina	16
Singapore	6	Greece	17
Mexico	7	China	18
Belgium	8	Hong Kong	19
Saudi Arabia	9	Thailand	20
United Kingdom	10	Macedonia	21
Spain	11	Brazil	22

Check system's status

The system's status may suggest problem areas. Refer to *Maintenance for Avaya MultiVantage and DEFINITY Server CSI* (555-233-119).

To access system's status:

1. Log into the system.
2. Enter **status system all-cabinets**.
3. Press Enter.
4. Verify that the screen displays the service state of **in** for every appropriate area.

Set up your system

You are now ready to follow procedures to start your system, including:

- Setting up dial plans, feature access codes (FACs), and extension ranges
- Adding extensions for users
- Setting up special features
- Setting up routing
- Assigning and changing users

See Configure Avaya Site Administration on page 7-10 to set up Avaya Site Administration.

For more information, see:

- *Avaya Communication Manager Little Instruction Book for Basic Administration* (555-233-756)
- *Avaya Communication Manager Little Instruction Book for Advanced Administration* (*555-233-757)*
- *Avaya Communication Manager Little Instruction Book for Basic Diagnostics* (555-233-758)
- *Administrator's Guide for Avaya Communication Manager* (555-233-506)

Set country options

Some country options need to be set to turn off the red alarm LEDs.

1. At the SAT or DSA window, type **change system-parameters country options** and press Enter. A screen similar to the following illustration displays on the terminal. The cursor is set on the `Companding Mode` field.

NOTE:
Be sure that there are no active AUDIX calls when you change the companding mode. If there are active AUDIX calls, those calls will suddenly have a very loud audio stream. The best way to ensure that there are no active AUDIX calls is to busy the CWY1 circuit pack (1A12) before you change the companding mode.

```
change system-parameters country-options                Page   1 of  21   SPE A
                      SYSTEM PARAMETERS COUNTRY-OPTIONS

            Companding Mode: Mu-Law            Base Tone Generator Set: 1
          440Hz PBX-dial Tone? n             440Hz Secondary-dial Tone? n
            Digital Loss Plan: 1
       Analog Ringing Cadence: 1     Set Layer 1 timer T1 to 30 seconds? n
    Analog Line Transmission: 1    Enhanced 84xx Display Character Set? n


TONE DETECTION PARAMETERS
          Tone Detection Mode: 6
             Interdigit Pause: short
```

2 The default (United States) companding mode is µ-Law. If the country uses A-Law companding, type A-Law. Press Enter when finished.

Administer the attendant console

1 Enter **display system-parameters country-options**. Verify the system's companding mode for its local stations (usually, A-Law for Europe and µ-Law for North America and Japan).

2 If necessary, enter **change terminal-parameters 603/302B1** to change the default system-level parameters and audio levels for these terminals.

> **NOTE:**
> For information about changing the default parameters and audio levels, refer to *DEFINITY Application Notes* available through the International Technical Assistance Center (ITAC).

3 Administer other forms listed under "Attendant Console" in *DEFINITY Enterprise Communications Server Release 7 Administrator's Guide*, 555-233-502.

Add translations

Refer to *Administrator's Guide for Avaya Communication Manager* (555-233-506) to add new terminals.

Administer telephone features

1. According to the customer's order, administer Communication Manager's translations, INTUITY AUDIX mailboxes, etc. in one of two ways:
   a. Avaya Site Administration (web)

      Avaya Site Administration must be installed on the laptop or on a remote PC that is connected to the S8100.

      Connect the PCMCIA card with the laptop or through remote PC using a web browser (Internet Explorer or Netscape).

   b. Avaya (Lucent) Access Control (LAC) [telnet]

      (For direct SAT access without going through Avaya Site Administration)

      Telnet to S8100 through the LAC to receive the SAT screen. See Start a Telnet session on page 162.

Place a test call

1. From any telephone connected to a Digital Line circuit pack, call any nearby telephone connected to an Analog Line circuit pack.
2. Verify that the dial tone, ringing pattern, and talk path are acceptable.
3. Place a call through the central office (outside call) to any nearby telephone.
4. Verify that the dial tone, ringing pattern, and talk path are acceptable.

Test INADS callout

From the SAT, run **test inads-link**.

Setup call-detail recording(CDR)

To ensure the proper collection of CDR/SMDR call records from the S8100 PBX when using the Collect from File Protocol, it is necessary to collect call records via a LAN connection between the S8100 server platform and the call-accounting client's platform. The following descibes administration of the network connections.

Before beginning, ensure that proper network connectivity exists between the S8100 server platform and the call-accounting client's platform. Also, ensure that call rating has been turned off in the call-accounting client, if the database has not yet been initialized.

A login for the call-accounting system has to be established in the S8100 Windows 2000 Server™ software. This is accomplished as follows, using either Terminal Server™ to access the system desktop, or a customer-supplied keyboard, mouse, and monitor:

1. Select Start, Programs, Administrative Tools (Common).
2. Click **Computer Management**.
3. Click **Local Users & Groups**.

4 Right-click **Users' folder**, then select **New User**.

5 In the dialog, assign the *Username* (this is the login) and *Password*.

> **NOTE:**
> The *Full Name and Description* are optional. The option check boxes are the customer's choice; however, we recommend that *User Cannot Change Password* and *Password Never Expires* should be the only ones checked.

6 Click **Groups** at the bottom of the dialog.

7 Make the login a member of *officeadmin* and *Users* groups and click **OK**.

8 Click **OK** in the **New User** dialog, then Close **Computer Management**.

Share CDR data

The following steps are for sharing the CDR data. This is set up via Terminal Server™ or the PC console to access the system desktop:

1 Right-click the My Computer icon on the desktop.

2 Select ***Explore***.

3 Click the + in front of the D: drive.

4 Click the + in front of LucentData.

5 Right-click the CDR folder, and select ***Sharing***.

6 Click ***Shared As***; leave the share name as *cdr.*

7 Click **OK**.

Map a shared CDR directory

At the call-accounting client's platform:

1 Using Windows Explorer, access Tools, Map Network Drive, and note the next available drive letter listed under *drive*.

2 Enter the machine name of the S8100 server platform and the shared CDR directory in the following example format (\\DEFONE\CDR); then click OK.

3 Enter User name and Password, click **OK**.

4 Check the left pane of the Explorer window to verify that a mapped entry such as CDR on 'Def1' F:\ is visible.

5 Click that entry to check for cas.in files if the S8100 is processing calls.

> **NOTE:**
> Any problems mapping this drive or accessing the shared CDR directory after mapping indicates a network connectivity or administration problem, and must be resolved before proceeding.

Set call-collection interface

1. Access the call accounting main menu, and select **Configuration Call Collection Interface**.
2. Select the *Collect from File 1.1* entry, under ***Protocol/Device used to collect call records***.
3. Ensure that a format has been set.

   NOTE:
   S8100 should be set to output 24-word (unformatted) call records.

4. Click **Configure Settings**.
5. Enter the drive letter of the previously mapped drive to the S8100 server, along with the file's name, cas.in (for example, F:\cas.in).
6. Ensure that a proper polling interval is displayed (the default of 60 seconds is usually fine); then click **OK** to save the settings.
7. Still in the **Configuration Call Collection Interface** dialog, ensure that the *enable from/to* entry is set to the **future**.
8. Click **Close**.

   The interface will restart.

Verify call-record collection

To verify call-record collection, click the protocol icon in the taskbar for the site being administered, and wait for call-record collection. Access Call Processing Status for CASW and enable rating only if the database has been initialized and the customer is ready to process calls.

If proper call records are being collected and processed, you have successfully administered call-record collection for this PBX and site.

NOTE:
There is no error checking from call accounting of the call-collection path, and no message log entries of any access errors. If call collection fails, check the network, administration, drive mapping, shared CDR folder, and path entries for resolution.

Call accounting

Call-accounting systems receive Call Detail Records (CDRs) from an S8100 system and process the information into management reports. The S8100's software writes CDRs to a CDR file and stores it in a CDR directory. The Avaya call-accounting systems are widely compatible and require little maintenance, even while collecting data, generating reports, and managing remote data-collection sites.

Avaya provides the following call-accounting products to help reduce telephone expenses, optimize resources, assign costs, identify abuse, and clearly understand telephone expenses and convey that understanding to others:

- **eCAS** – A totally web-based call-accounting system supporting general businesses with from 25 to 20,000 extensions at up to 100 locations.
- **eCAS Lite** – A reduced-feature version of eCAS supporting small businesses with up to 100 extensions.
- **INTUITY™ Call Accounting** – Fully integrated on the INTUITY platform supporting small S8100 and MERLIN LEGEND® customers.
- **Quantum Series** – A suite of telemanagement applications including the Call-Master Call-Accounting system.
- **Infortel for Windows Lodging** – Interfaces with most Property Management Systems (PMS) to provide PC-based telemanagement for the Lodging industry.

Call-accounting systems need full read and write permissions to access the S8100 CDR files and directories across the network.

Setting up call-accounting access will vary depending on the customer's specific network. See the system/network administrator to ensure that proper permissions are set up for the file and directory. More information about these products, including installation and training offers, can be found on the Avaya Support web site under Products and Services.

Administer Communication Manager for INTUITY AUDIX initialization

Check the dial plan

The dial plan tells the system how to interpret dialed digits and how many digits to expect for certain calls. For example, if a 9 is dialed to access an outside line, the dial plan tells the system to find an external trunk for a dialed string beginning with 9.

To check the dial plan:

1. At the SAT or Avaya Site Administration window, enter **disp dialplan analysis**.

   The Dial Plan Analysis Table form displays. Make note of the extension lengths for the ext Call Types. The number of digits can only be changed through the web interface.

2. Press F1 to cancel the command.

3 Enter **display dialplan parameters**.

The Dial Plan Parameters form displays, which should have the correct local node number:

```
display dialplan parameters
                              DIAL PLAN PARAMETERS

                 Local Node Number: 1
                   ETA Node Number:
               ETA Routing Pattern:
        UDP Extension Search Order: local-extensions-first
  6-Digit Extension Display Format: xx.xx.xx
  7-Digit Extension Display Format: xxx-xxxx
       AAR/ARS Internal Call Prefix:
AAR/ARS Internal Call Total Length:

Command:
```

4 Make note of the local node number (first digit). The local node number can only be changed through the web interface.

5 Press F1 to cancel the command.

Check hunt groups

1 At the SAT or Avaya Site Administration window, type **list hunt group**.

The Hunt Groups form displays:

```
list hunt-group group

                                   HUNT GROUPS
Grp Grp
No. Name/            Grp     ACD/          Que No. Cou  Notif/  Dom   Message
    Ext              Type    MEAS Vec MCH  Siz Mem Path Ctg Adj Ctrl  Center

1   monroe voice hunt
    2000             ucd-mia n/-  n   none 8   8        n             A
2   paradox voice hunt
    2600             ucd-mia n/-  n   none 8   8        n             n
3   rockville voice hunt
    2650             ucd-mia n/-  n   none 6   8        n             n

Command successfully completed
Command:
```

2 Note the following information about the INTUITY AUDIX hunt group:

- Grp No.
- Grp Name/Ext.

3 Press F1 to cancel the command.

Check class of service

1 At the SAT or Avaya Site Administration window, type **disp cos**.

The Class of Service form displays:

```
display cos
                                CLASS OF SERVICE

                                0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15

 Auto Callback                  n  y  y  n  y  n  y  n  y  n  y  n  y  n  y  n
 Call Fwd-All Calls             n  y  n  y  y  n  n  y  y  n  n  y  y  n  n  y
 Data Privacy                   n  y  n  n  n  y  y  y  y  n  n  n  n  y  y  y
 Priority Calling               n  y  n  n  n  n  n  n  n  y  y  y  y  y  y  y
 Console Permissions            n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Off-hook Alert                 n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Client Room                    n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Restrict Call Fwd-Off Net      y  y  y  y  y  y  y  y  y  y  y  y  y  y  y  y
 Call Forwarding Busy/DA        n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Personal Station Access (PSA)  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Extended Forwarding All        n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Extended Forwarding B/DA       n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Trk-to-Trk Transfer Override   n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 QSIG Call Offer Originations   n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n

Command:
```

2 Find the COS you plan to use for the INTUITY AUDIX port stations. It is usually COS 5.

3 Ensure that Data Privacy and Restrict Call Fwd-Off Net are set to **y**.

4 Ensure the other fields are set to **n**.

5 Press F1 to cancel the command.

Check class of restriction

1 At the SAT or Avaya Site Administration window, type **disp cor 1**, where **1** is the COR you plan to use for the INTUITY AUDIX port stations.

The Class of Restriction form displays:

```
display cor 1                                                  Page   1 of   4
                                CLASS OF RESTRICTION

                COR Number: 1
           COR Description: audix

                      FRL: 7                                APLT? y
  Can Be Service Observed? n           Calling Party Restriction: none
Can Be A Service Observer? n            Called Party Restriction: none
        Time of Day Chart: 1       Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? n
     Restriction Override: none       Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n

            Access to MCT? y            Fully Restricted Service? n
     Category For MFC ANI: 7
         Send ANI for MFE? n
            MF ANI Prefix:              Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                        Can Be Picked Up By Directed Call Pickup? n
                                    Can Use Directed Call Pickup? n
                                    Group Controlled Restriction: inactive
```

2 Ensure that the COR has an FRL of **7** to allow for Outcalling and Fax Print.

3 Ensure that Calling Party Restriction is set to **none**.

4 Ensure that Time of Day Chart is set to **1**.

5 Press F7 to go to the next page of the form.

Page 2 of the Class of Restriction form displays.

6 Press F7 to go to the next page of the form.

Page 3 of the Class of Restriction form displays:

```
display cor 1                                              Page   3 of   4
                            CLASS OF RESTRICTION

CALLING PERMISSION (Enter "y" to grant permission to call specified COR)

  0? y     12? y     24? y     36? y     48? y     60? y     72? y     84? y
  1? y     13? y     25? y     37? y     49? y     61? y     73? y     85? y
  2? y     14? y     26? y     38? y     50? y     62? y     74? y     86? y
  3? y     15? y     27? y     39? y     51? y     63? y     75? y     87? y
  4? y     16? y     28? y     40? y     52? y     64? y     76? y     88? y
  5? y     17? y     29? y     41? y     53? y     65? y     77? y     89? y
  6? y     18? y     30? y     42? y     54? y     66? y     78? y     90? y
  7? y     19? y     31? y     43? y     55? y     67? y     79? y     91? y
  8? y     20? y     32? y     44? y     56? y     68? y     80? y     92? y
  9? y     21? y     33? y     45? y     57? y     69? y     81? y     93? y
 10? y     22? y     34? y     46? y     58? y     70? y     82? y     94? y
 11? y     23? y     35? y     47? y     59? y     71? y     83? y     95? y
```

7 Ensure that every field is set to **y** so there are no restrictions.

> **NOTE:**
> Pay attention to toll fraud issues.

8 Press F1 to cancel the command.

Change the dial plan

To change the dial plan:

1 Type **change dialplan analysis**.

The Dial Plan Analysis Table screen displays:

```
change dialplan analysis                    Page   1 of   1

              DIAL PLAN ANALYSIS TABLE
                                                  Percent Full: 20

  Dialed Total  Call    Dialed Total  Call    Dialed Total  Call
  String Length Type    String Length Type    String Length Type
    0      1    attd
    3      4    ext
    4      4    ext
    5      6    ext
    7      3    dac
    8      1    fac
    *      3    fac
```

2 For example, to define 3000 – 3999 as an extension range:

   a type **3** in the `Dialed String` column

   b in the same row, type **4** in the `Total Length` column

   c type **ext** in the `Call Type` column

3 For example, to specify that the range 700 – 799 is to be used for dial access codes:

   a type **7** in the `Dialed String` column

   b in the same row, type **3** in the `Total Length` column

   c type **dac** in the `Call Type` column

4 Submit the form to save your changes.

Add AUDIX ports

Stations are added by entering a **change machine** command with the starting and ending numbers (for example, 0000 – 9999 starting and ending range for a 4-digit extension length).

> **NOTE:**
> Check the Dialplan Analysis Table for the correct extension lengths.

To set up stations for INTUITY AUDIX ports:

1 At the SAT or Avaya Site Administration window, enter **add sta <number>**, where **number** is the station you want to use for the first INTUITY AUDIX port.

   The Station form displays:

```
add station 2001                                          Page   1 of   4
                                  STATION

Extension: 2001                         Lock Messages? n          BCC: 0
     Type:                              Security Code:             TN: 1
     Port:                            Coverage Path 1:             COR: 2
     Name:                            Coverage Path 2:             COS: 5
                                      Hunt-to Station:

STATION OPTIONS
             Loss Group: 2                 Personalized Ringing Pattern: 1
           Data Module? n                           Message Lamp Ext: 2017
         Speakerphone: 2-way                     Mute Button Enabled? y
       Display Language: english

                                                  Media Complex Ext:
                                                        IP SoftPhone? n
                                                 Remote Office Phone? n
```

2 Type **2500** in the Type field.

3 Type **01A1201** in the Port field. This is a virtual port used to communicate between Communication Manager and INTUITY AUDIX.

4 Type a name in the Name field.

5 Enter the correct COR and COS.

6 Press F7 to go to the next page.

Page 2 of the Station form displays:

```
add station next                                          Page   2 of   4
                                    STATION
FEATURE OPTIONS
           LWC Reception: msa-spe
          LWC Activation? n                      Coverage Msg Retrieval? n
  LWC Log External Calls? n                                Auto Answer: none
             CDR Privacy? n                           Data Restriction? n
   Redirect Notification? n                      Call Waiting Indication? n
 Per Button Ring Control? n                  Att. Call Waiting Indication? n
   Bridged Call Alerting? n                     Distinctive Audible Alert? n
       Switchhook Flash?: y                           Adjunct Supervision? y
    Ignore Rotary Digits? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: basic                  Audible Message Waiting? n
    MWI Served User Type:

                                                Coverage After Forwarding? s
                                                  Multimedia Early Answer? n
                                          Direct IP-IP Audio Connections? n
  Emergency Location Ext: 2002                      IP Audio Hairpinning? n
```

7 Type **audix** in the `LWC Reception` field.

8 Ensure that every other field, except for Switchhook Flash and Adjunct Supervision, are set to **n**.

9 Press F7 to go to the next page.

Page 3 of the Station form displays:

```
add station next                                          Page   3 of   4
                                    STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                         Mounting: d
      Floor:                                       Cord Length: 0
   Building:                                         Set Color:




ABBREVIATED DIALING
     List1:                    List2:                    List3:

HOT LINE DESTINATION
          Abbreviated Dialin List Number (From above 1, 2, or 3):
                                                       Dial Code:

      Line Appearance: call-appr
```

10 Ensure that `Line Appearance` is set to **call-appr**.

11 Submit the form.

12 Type **duplicate station <number>**, where **number** is the station you set up for the first INTUITY AUDIX port.

The Duplicate Station form displays:

```
duplicate station 2001                                    Page   3 of   4
                                    STATION

Ext      Port    Name                        Security
                                             Code    Room     Jack   Cable
1001     01A1201
```

13 Add the 7 remaining stations (for example, Ext 2002 to Port 01A1202, Ext 2003 to Port 01A1203, etc.)

This allows you to add every station at the same time on the same form.

Make a hunt group

1 At the SAT or Avaya Site Administration window, type **add hunt next**.

The Hunt Group form displays:

```
add hunt-group next                                          Page   1 of  10
                                HUNT GROUP

            Group Number: 1                                 ACD? n
              Group Name:                                 Queue? n
         Group Extension:                                Vector? n
              Group Type: ucd-mia                Coverage Path:
                      TN: 1          Night Service Destination:
                     COR: 1                    MM Early Answer? n
           Security Code:
     ISDN Caller Display:
```

2 Note the `Group Number`.

3 Type a name in the `Group Name` field.

4 Type the Group Extension.

5 Ensure that `Group Type` is set to **ucd-mia**.

6 Ensure that `Queue` is **y** and `Queue Length` is **8**.

7 Press F7 to go to the next page of the form.

The Hunt Group form displays:

```
add hunt-group next                                          Page   2 of  10
                                HUNT GROUP

                           Message Center: audix




    Calling Party Number to INTUITY AUDIX? n
                            LWC Reception: none
```

8 Ensure that `Message Center` is set to **`audix`**.

9 Press Tab. The `Calling Party Number to INTUITY AUDIX` field appears. Ensure that this field is set to **n**.

10 Ensure that LWC Reception is set to **none**.

11 Press F7 to go to the next page of the form.

Page 3 of the Hunt Group form displays:

```
add hunt-group next                                          Page   3 of  10
                                HUNT GROUP
          Group Number: 4       Group Extension: 2900        Group Type: ucd-mia
  Member Range Allowed: 1 - 200          Administered Members (min/max): 0  /0
                                             Total Administered Members: 0
GROUP MEMBER ASSIGNMENTS
     Ext   Name                                Ext   Name
  1: 2001                                 14: _____
  2: 2002                                 15: _____
  3: 2003                                 16: _____
  4: 2004                                 17: _____
  5: 2005                                 18: _____
  6: 2006                                 19: _____
  7: 2007                                 20: _____
  8: 2008                                 21: _____
  9: _____                                22: _____
 10: _____                                23: _____
 11: _____                                24: _____
 12: _____                                25: _____
 13: _____                                26: _____

  At End of Member List
```

12 Type the extensions of the 8 stations you entered before.

13 Press F3 to submit the changes.

Change coverage path

1 At the SAT or Avaya Site Administration window, type **add cov pa 2**.

The Coverage Path form.displays:

```
add coverage path 2                                          Page   1 of   1
                                COVERAGE PATH

                 Coverage Path Number: 2
                                                 Hunt after Coverage? n
                     Next Path Number: ____      Linkage

COVERAGE CRITERIA

    Station/Group Status    Inside Call     Outside Call
              Active?           n               n
                Busy?           y               y
      Don't Answer?             y               y          Number of Rings: 3
                 All?           n               n
 DND/SAC/Goto Cover?            y               y

COVERAGE POINTS

    Terminate to Coverage Pts. with Bridged Appearances? n

      Point1: h4_____           Point2: ______          Point3: ______
      Point4: ______            Point5: ______          Point6: ______
```

2 Ensure that `Number of Rings` is set to **3**.

3 Ensure that `Point1` is set to the INTUITY AUDIX hunt group that you previously set up.

4 Submit the form.

Add test phones

1 At the SAT or Avaya Site Administration window, type **add sta next**.

```
add station next                                          Page   1 of   4
                                  STATION

Extension: 2017                          Lock Messages? n          BCC: 0
     Type: 6408D+                      Security Code:            TN: 1
     Port:                            Coverage Path 1:           COR: 1
     Name:                            Coverage Path 2:           COS: 1
                                       Hunt-to Station:

STATION OPTIONS
             Loss Group: 2                Personalized Ringing Pattern: 1
           Data Module? n                         Message Lamp Ext: 2017
           Speakerphone: 2-way                     Mute Button Enabled? y
       Display Language: english

                                                  Media Complex Ext:
                                                          IP SoftPhone? n
                                                   Remote Office Phone? n
```

2 Type the kind of phone you are using in the `Type` field.

3 Type the port in the `Port` field.

4 In the `Coverage Path 1` field, type the number of the coverage path you just created or changed.

5 Fill in any other appropriate fields and submit the form.

Save translations

1. Enter **save translation**, and press Enter. This instructs the system to take all translation information in memory and write it to the translation cards.
2. Update backup cards, if necessary.

INTUITY AUDIX administration

This section provides information about INTUITY AUDIX commands and administering INTUITY AUDIX. For additional information about INTUITY AUDIX administration, refer to the *AUDIX Administration PDF files* on the Documentation CD and *DEFINITY ONE Communications System AUDIX Administration Command Line Quick Reference* Card (555-233-737).

INTUITY AUDIX commands

Commands available to change system settings and subscriber information in the INTUITY AUDIX application are executable from the INTUITY AUDIX command prompt. You can access the INTUITY AUDIX command prompt from the Avaya Site Administration or Telnet interface. To view a list of commands, press F6 (or press the “choices” tab). The following INTUITY AUDIX screen displays:

```
monroe              Active          Alarms: none                  Logins: 1

-add     to enter new administrative records
 audit   to validate system data
 change  to modify existing administrative records
 copy    to copy announcements and fragments
 display to display administrative records and maintenance logs
 exit    to exit from AUDIX administration and maintenance
 get     to request remote updates
 help    to display available types of help
 list    to produce reports
 logoff  to log off the system
 print   to send the command output to the attached printer
 remove  to remove administrative records
 reset   to restart or shutdown the Messaging Core
 test    to test alarm origination or outcall
 toggle  to toggle the function key settings
 trace   to turn on amis trace

enter command:
```

Adding an INTUITY AUDIX subscriber

After completing the machine level translations, subscribers must be added to the S8100 system. The following forms detail the addition of INTUITY AUDIX subscribers. Enable the INTUITY AUDIX forms via Avaya Site Administration or Telnet.

1. Start at the INTUITY AUDIX command prompt.
2. Enter the command **Add Subscriber** and the extension number that the new subscriber will use.

3 Enter the data for the subscriber on page 1 of the Add Subscriber form as detailed in Table 27, Field definitions for Add Subscriber screen, page 1, on page 195.

The Add Subscriber form, page 1 displays:

```
monroe             Active          Alarms:   wA                      Logins: 1
add subscriber 2600                                                Page 1 of 2
                                  SUBSCRIBER

         Name: Jones, John                          Locked? n
    Extension: 2600                                Password:
          COS: class01                        Miscellaneous 1:
Switch Number:                                Miscellaneous 2:
 Community ID:                                Miscellaneous 3:
Secondary Ext:                                Miscellaneous 4:
 Account Code:                              Covering Extension:
                                             Broadcast Mailbox?

Email Address:



Press [ENTER] to execute or press [CANCEL] to abort
enter command: add subscriber 2600
```

Table 27: Field definitions for Add Subscriber screen, page 1

Field	Valid input	Description
Name	Subscriber's Name	This is the name of the subscriber. In the example above: Jones, John
Extension	Extension number	This is the extension number assigned on Communication Manager for the subscriber.
Password	Can be alpha or numeric	Subscriber's password. Input a temporary password and instruct the new subscriber to change their password when they log into INTUITY AUDIX.
COS	class00 to class11	Class of service; contains features that an INTUITY AUDIX subscriber could be enabled to use. Set up the Class of Service on the system before adding subscribers.

4 Press F3 to save the information.

When adding subscribers to INTUITY AUDIX, the preferred method is to first set up a Class of Service (COS) for a group of INTUITY AUDIX subscribers. Using this method, the data is filled in for you on page 2 of the Add Subscriber form. The following is an example of page 2 of the Add Subscriber form.

TheAdd Subscriber Form, page 2 displays:

```
monroe             Active           Alarms:   wA                       Logins: 1
add subscriber 2600                                                  Page 2 of 2
                       SUBSCRIBER CLASS OF SERVICE PARAMETERS
 Addressing Format: extension             Login Announcement Set: System
 System Multilingual is OFF         Call Answer Primary Annc. Set: System
 Call Answer Language Choice? n  Call Answer Secondary Annc. Set: System

PERMISSIONS
      Type: call-answer     Announcement Control? n             Outcalling? n
      Priority Messages? y              Broadcast: none        IMAPI Access? y
 IMAPI Message Transfer? y          Fax Creation? y  Trusted Server Access? y

INCOMING MAILBOX          Order: fifo               Category Order: nuo
  Retention Times (days),   New: 10       Old: 10         Unopened: 10
OUTGOING MAILBOX          Order: fifo               Category Order: unfda
Retention Times(days), File Cab: 10       Delivered/Nondeliverable: 10

Voice Mail Message (seconds),  Maximum Length: 1200 Minimum Needed: 32
Call Answer Message (seconds), Maximum Length: 1200 Minimum Needed: 8
        End of Message Warning Time (seconds):
          Maximum Mailing Lists: 25     Total Entries in all Lists: 250
Mailbox Size (seconds), Maximum: 1200            Minimum Guarantee: 0
Press [ENTER] to execute or press [CANCEL] to abort
enter command: add subscriber 2600
```

Download Avaya Site Administration

Avaya Site Administration is a purchase option with the Avaya Integrated Management Suite. Avaya Site Administration is available for download as described in this section only if the customer has purchased the appropriate option. See Chapter 7, "Avaya Site Administration" for more information about Avaya Site Administration.

NOTE:
The IP address differs according to the type of physical connection established.

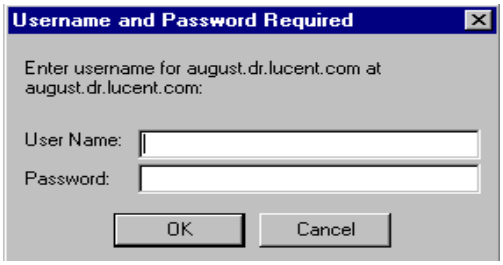
1 Open an Internet browser.

2 Type **http:// <IP address>** in the address area of the web browser.

The home page displays:

3 Click **Administer System**.

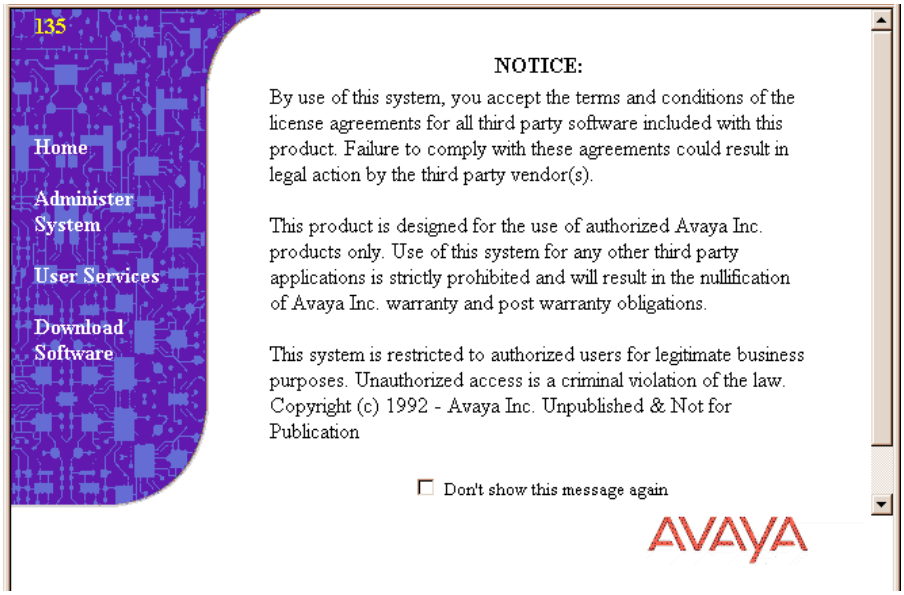
A dialog similar to the following displays:



4 Type the user name and password.

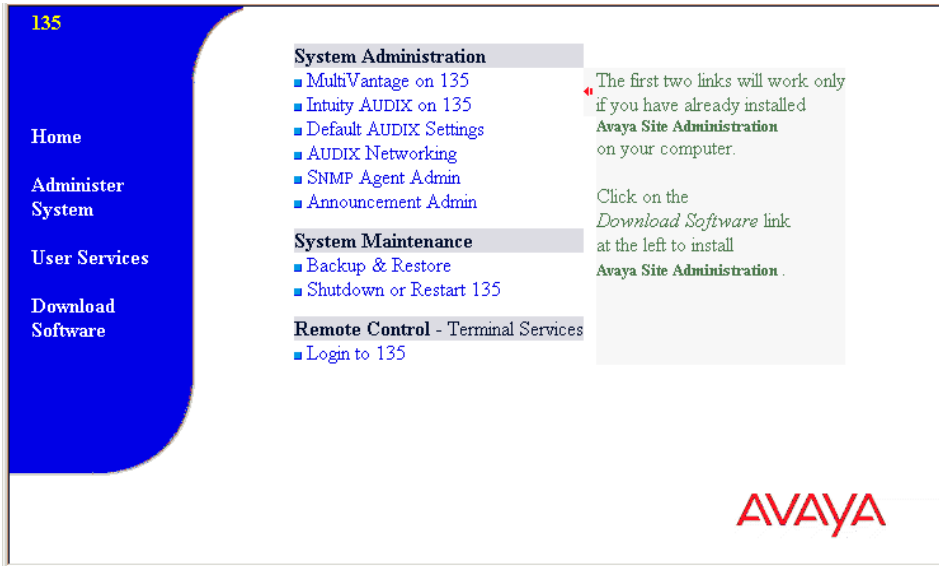
NOTE:
The Avaya Services representative uses the logins **lucent1**, **lucent2**, or **lucent3** and either the LAC password (NT password) or the ASG challenge. The customer uses an appropriate password to log in, such as NTadmin.

The following page displays:



5 After reading the page, click **Continue**.

A page similar to the following displays:



6 Click **Download Software.**

The **Software Download** page displays.

7 Click **Avaya Site Administration**.

The **Save As** dialog displays.

8 Choose a destination, such as the desktop.

The **Locations Saved To** page displays. When Avaya Site Administration, is saved, it reverts to the **Software Download** page.

9 Double-click the application name in the directory where you saved it.

The **Unpacking Avaya Site Administration** dialog and a **Welcome** dialog are displayed.

10 Click **Next**.

The Avaya Site Administration dialog, including installation and related information, displays:

11 Click **Next**.

12 Click **Finish** when the “please wait” message disappears.

The Avaya Site Administration README file displays. Avaya Site Administration is installed on your PC and an Avaya Site Administration icon appears under **Start** → **Programs** → **Avaya Site Administration**.

Start an Avaya Site Administration session

Avaya Site Administration can be started as a normal application from Windows at the start button. To start an Avaya Site Administration session:

1 Open an Internet browser.

2 Type **http:// <IP address>** in the address area of the web browser.

The S8100 home page displays.

3 Navigate to the S8100 System Administration page, as in the previous section.

4 Click **INTUITY AUDIX** on **<machine name>** in the right pane.

Avaya Site Administration is launched.

5 Set up daily automatic backups of INTUITY AUDIX. Backups can be to the LAN, PCMCIA card, or preferably, to a directory on your server. See From the backup and restore main menu, you can: on page 307.

Administer SNMP

The SNMP agent is installed with S8100. By default, SNMP is enabled. See Enable and disable SNMP on page 178 for more information about enabling and disabling SNMP.

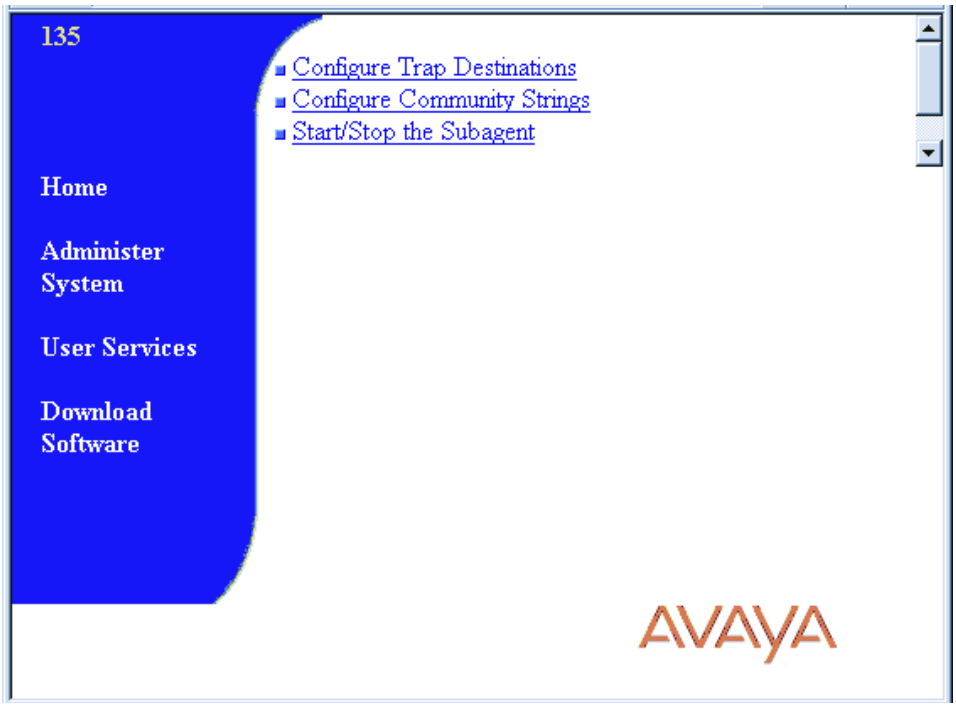
You can configure SNMP trap destinations, configure community strings, and start and stop the SNMP subagent process. After the SNMP agent is configured, and with Network Management System Interface (NMSI) software installed, a network manager can monitor S8100 devices. The NMSI software can automatically discover the S8100 devices in the network and display icons for them in an NMS IP map.

Configure SNMP trap destinations

To configure SNMP trap destinations:

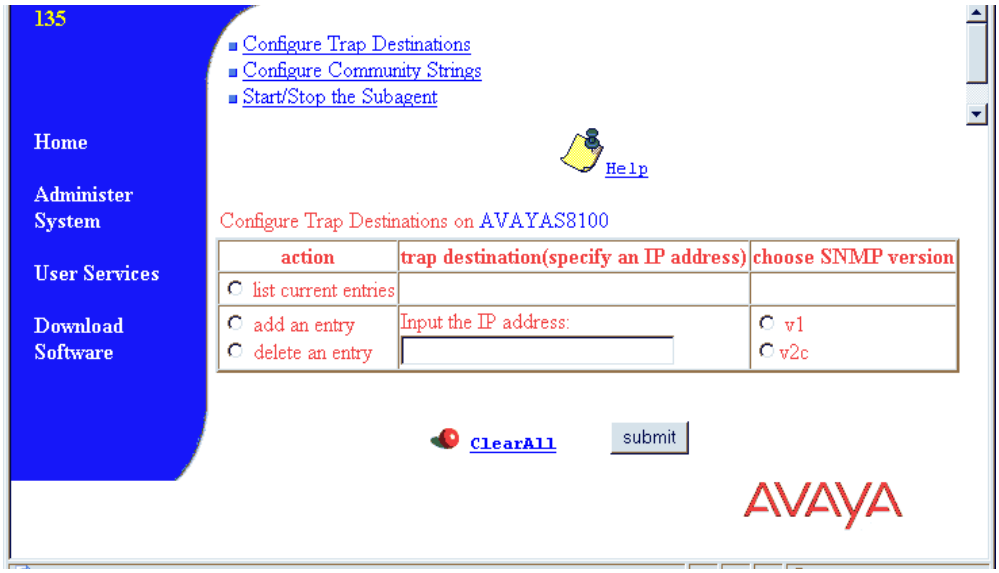
1. From the S8100 System Administration page, click **SNMP Agent Administration**.

   The following page displays:

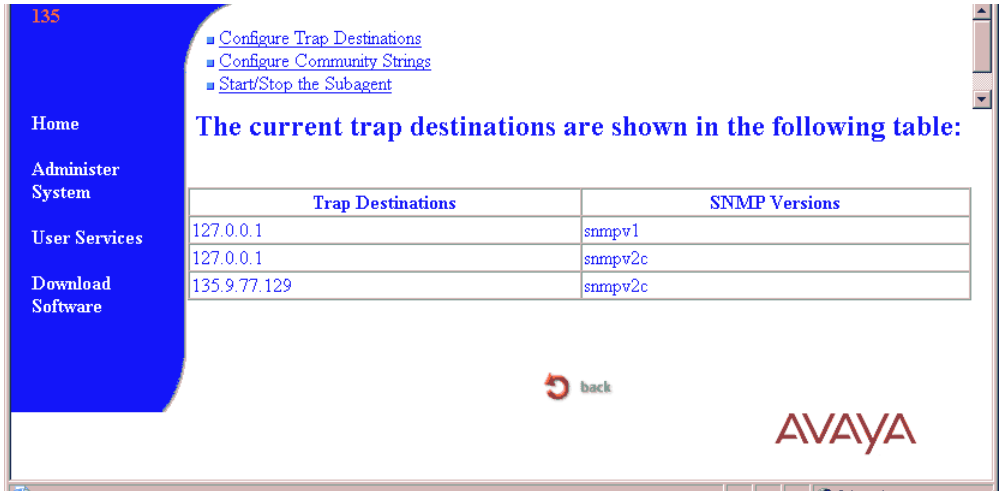


2. Click **Configure Trap Destinations**.

   The following page displays:



3 To list every current trap destination, choose the **list current entries** option and click the **Submit** button. The following page displays:



4 Click **Back** to return to the **Configure Trap Destinations** page.

5 To add an IP address to which traps are sent:

- **a** Choose the **add an entry** option.
- **b** Enter the IP address in the **Input the IP address** field.
- **c** Specify the SNMP version by clicking either the **V1** or **V2c** option.
- **d** Click **Submit**.

6 To delete an IP address:

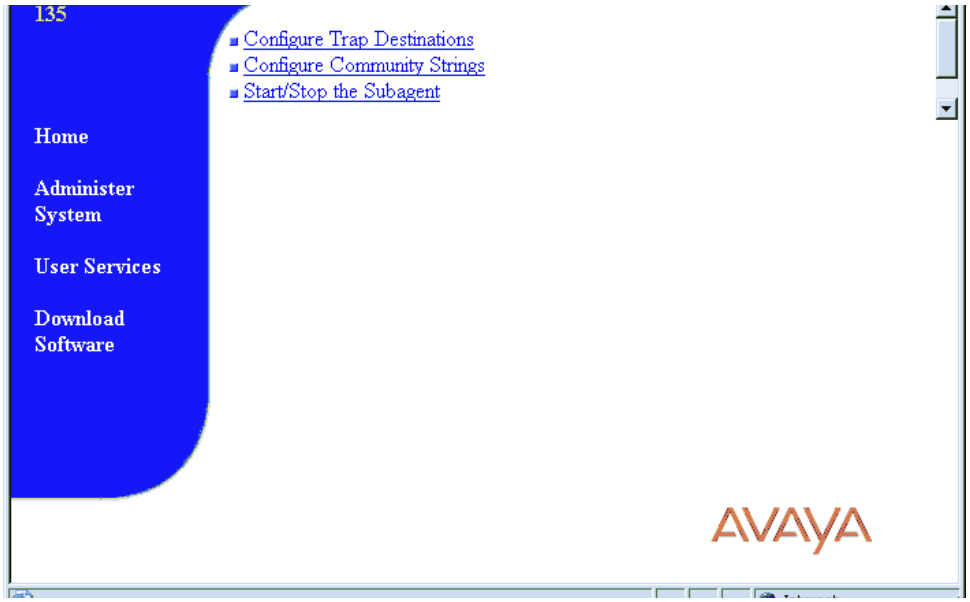
- **a** Choose the **delete an entry** option.
- **b** Enter the IP address in the **Input the IP address** field.
- **c** Click **Submit**.

Configure SNMP community strings

To configure community strings:

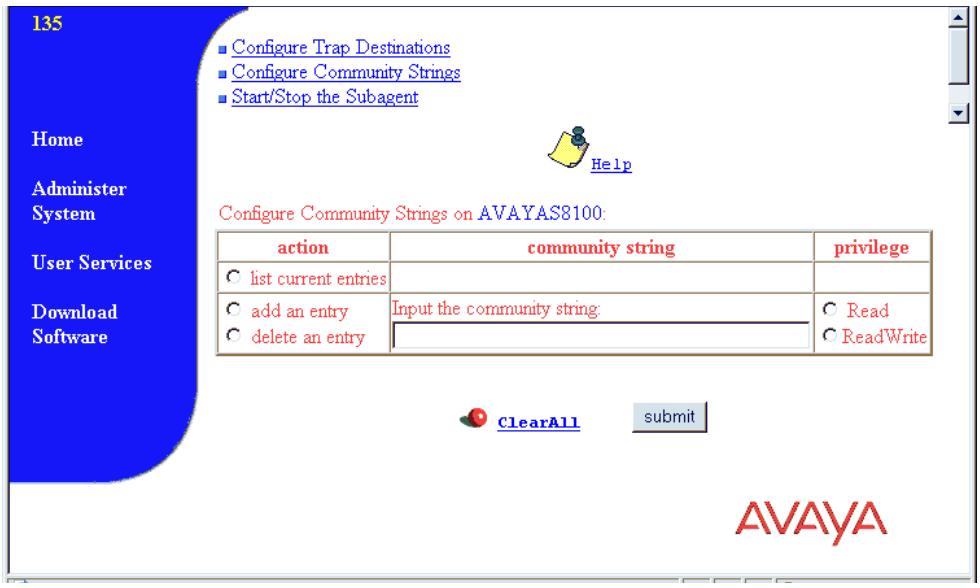
1. From the S8100 home page, click **SNMP Agent Administration**.

   The following page displays:



2. Click **Configure Community Strings**.

   The following page displays:



3 To list the currently administered community strings, click the **list current entries** option and click the **Submit** button.

The following page displays:

4 Click **Back** to return to the **Configure Community Strings** page.

5 To add a community string:

- **a** Click the **add an entry** option.
- **b** Enter the value in the **Input the community string** field.
- **c** Specify access permission by clicking the **Read** or **ReadWrite** options.
- **d** Click the **Submit** button.

6 To delete a community string:

- **a** Click the **delete an entry** option.
- **b** Enter the value in the **Input the community string** field.
- **c** Click the **Submit** button.

Start and stop SNMP

You can start and stop SNMP by using a bash command or the web interface.

To start SNMP using a bash command, start a bash session and enter **start snmp**. To stop SNMP using a bash command, start a bash session and enter **stop snmp**.

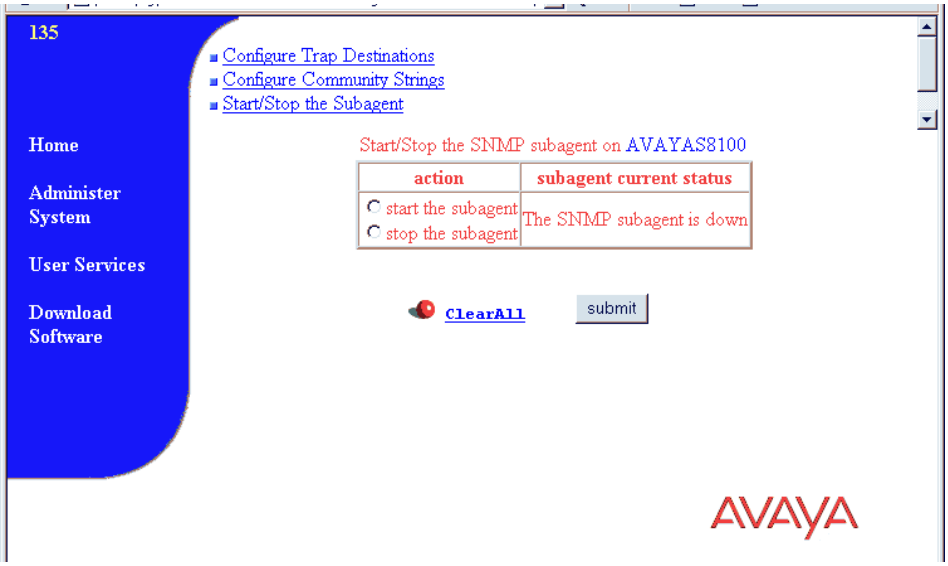
To start and stop SNMP using the web interface:

1. From the S8100 System Administration page, click **SNMP Agent Administration**.

   The following page displays

2. Click **Start/Stop the Subagent**.

   The following page displays:



   The **Start/Stop the Subagent** page shows whether the subagent process is running. From this page, you can start or stop the subagent process.

3. To start the subagent process, choose the **start the subagent** option and click **Submit**.

   To stop the subagent process, choose the **stop the subagent** option and click **Submit**.

Schedule backups

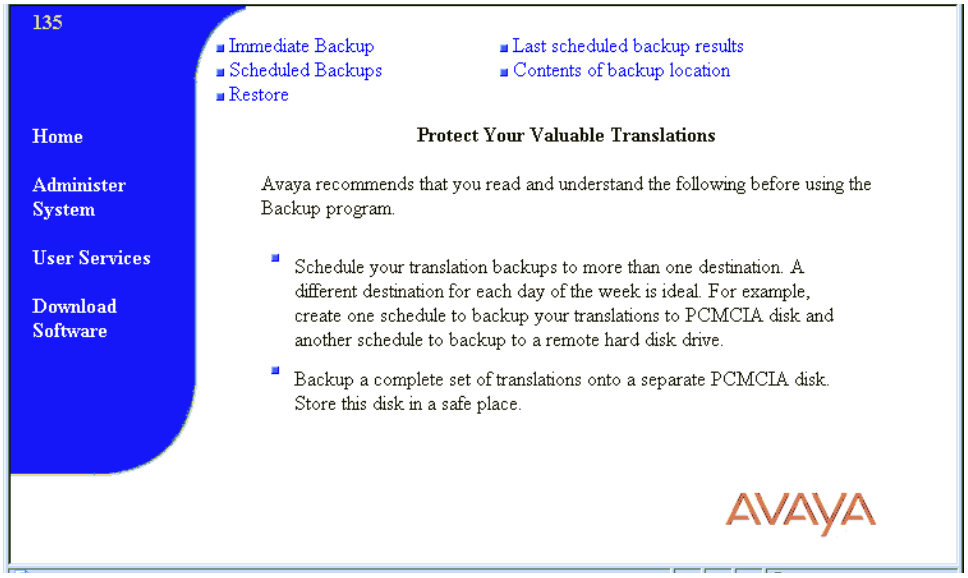
Backup procedures prevent loss of data due to system errors. Backups can be either immediate or scheduled. You can execute backup procedures to either the LAN or the PCMCIA flash card from the command line and web browser. For information about performing backups, see Perform backup on page 302.

NOTE:
Avaya strongly recommends that you schedule backups to more than one destination. For example, create one schedule to backup translations to a PCMCIA flash card and another schedule to backup to a different location for each day of the week on a remote hard disk drive on the LAN.

Add a scheduled backup

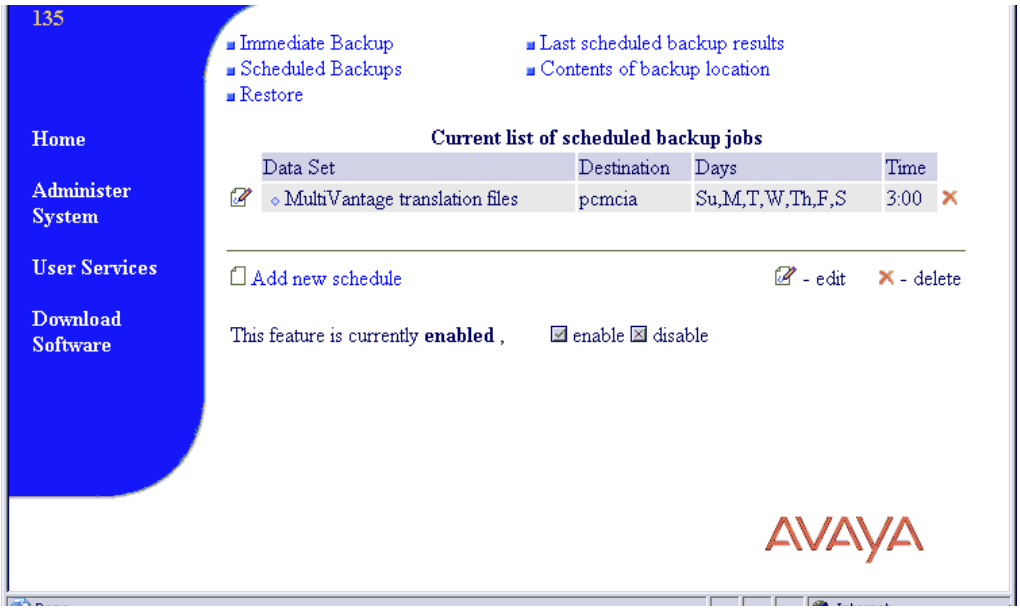
To schedule backups:

1. From the S8100 administration page, click **Backup and Restore** to open the main backup menu. The following page displays:



2 Click **Scheduled Backups**.

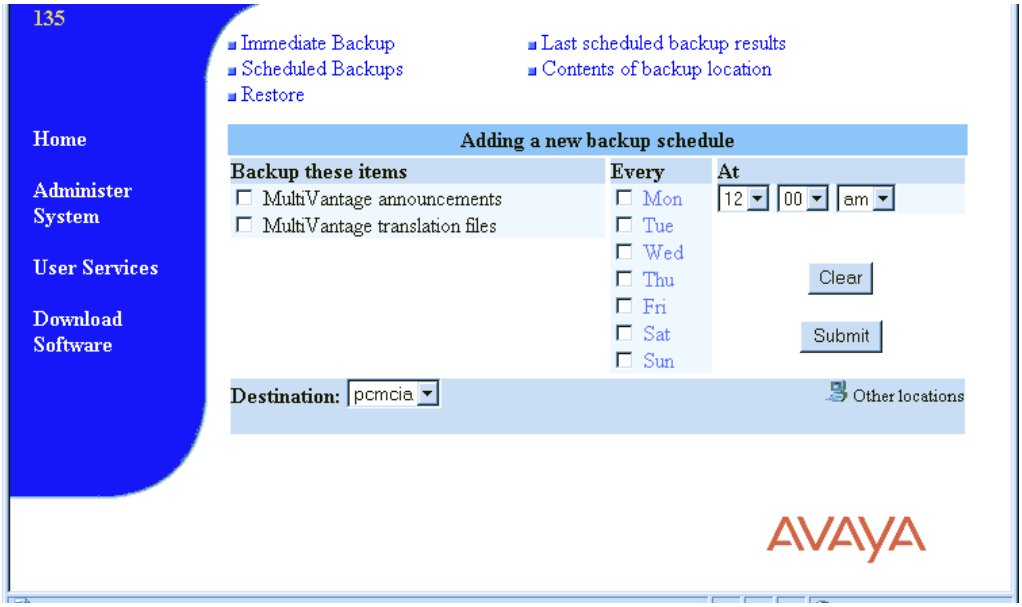
The following page displays:



From this page, you can add, edit, or delete scheduled backups.

3 On the **Current list of scheduled backup jobs** page, click **Add new schedule**.

The following page displays:



4 Select backup destination either to a LAN address or a PCMCIA Flash Disk.

5 Select items for scheduled backup.

6 Select a day and time for the backup.

7 Click **Submit**.

4 INTUITY AUDIX digital networking

This chapter provides information to administer digital networking after the S8100's initial system administration is finished. For further information, see *INTUITY AUDIX Administration.*

This chapter is organized as follows:

- Initial administration tasks on page 207
- View the Feature Options window on page 209
- Change number of administered remote users on page 210
- Administer networking channels on page 211
- Change local machine's information on page 212
- Add a remote machine on page 216
- Perform a full remote update on page 223
- Reset automatic deletion of nonadministered remote users on page 223
- View remote extensions on page 224

Initial administration tasks

To perform initial administration, complete the tasks shown in sequential order in Table 28, Initial administration tasks, on page 208. Confirm that each of the tasks are performed, as some may have been completed by the technician at installation.

The design center provides information for completing digital networking administration. Ensure that you have design center specifications for TCP/IP, network channels, the local machine, and every remote machine

Table 28: Initial administration tasks ***1 of 2***

Task	Description	Screens, windows, or commands
Complete Windows and switch administration (normally done by the technician at the time of installation).	Define the machine name, TCP/IP address, and the switch to work with AUDIX digital networking.	Windows Settings screens and Switch screens
View digital networking settings. See View the Feature Options window on page 209.	Verify that the purchased digital networking options are correctly displayed.	List Configuration window
Verify or change the number of administered remote users (normally done by the technician at the time of installation). See Change number of administered remote users on page 210.	Define the number of administered remote users as ≥ the number of mailboxes on every remote system.	System Parameters Limits screen
Administer network channels (normally done by the technician at the time of installation). See Administer networking channels on page 211.	Enable the channels to create a communication link between the ACCX card and the switch or the LAN card and the LAN.	Networking Channel Administration window
Change the local machine. See Change local machine's information on page 212.	Define local machine information for digital networking.	Machine Profile screen; Local Machine Administration window
Add a remote machine or change a remote machine (normally done by the technician at the time of installation). See Add a remote machine on page 216.	On the local machine, define information about each remote machine, including the machine name, password, connection type, and dial string.	Digital Machine Administration window; Machine Profile screen
Administer the AUDIX system on the remote machines.	On each remote machine, define information about the local machine.	Remote Machine Profile screen of the remote machine
Perform a full remote update. See Perform a full remote update on page 223.	Manually run a remote update for each remote machine to bring the network up to date immediately.	**get remote update** command

1 of 2

Table 28: Initial administration tasks ***2 of 2***

Task	Description	Screens, windows, or commands
Set automatic deletion of nonadministered remote users. See Reset automatic deletion of nonadministered remote users on page 223.	Sets the system to delete nonadministered remote users automatically.	System Parameters Features screen
View remote extensions. See View remote extensions on page 224.	Check that remote users were added to the local database.	List Remote Extensions screen
Record remote machine names.	Record the names of remote systems so that local users hear voiced confirmations when addressing messages to users on those remote systems.	Use the telephone to perform this task.

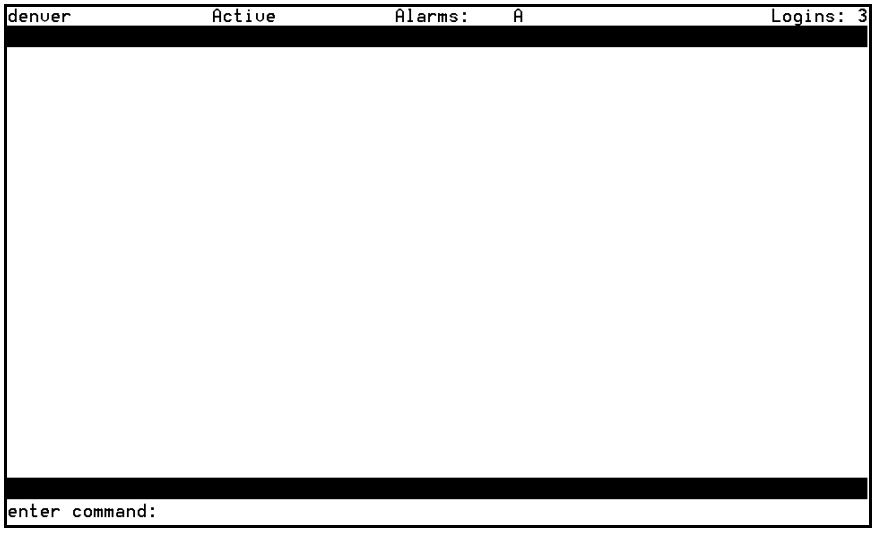
2 of 2

View the Feature Options window

View the Feature Options window to see the purchased options for digital networking. This window is display only, and can be changed only by Avaya-certified personnel.

To display the Feature Options window:

1. Start at the AUDIX Command Prompt screen, which displays as follows.



2 At the `enter command:` prompt, enter **list configuration**

The List Configuration screen displays:

```
hessville          Active          Alarms: M                    Logins: 1
list configuration                                               Page 1
                              LIST CONFIGURATION

                    Configuration Option              Value

          Audix Application                           ON
          DCS                                         ON
          Fax                                         ON
          High speed digital ports                    N/A
          Low speed digital ports                     N/A
          Max Number of IMAPI Sessions                6
          Multilingual                                ON
          SCSI Disk Mirroring                         N/A
          TCPIP digital ports                         1
          Text-to-Speech Sessions                     2
          Trusted Servers                             6
          hours_of_speech                             30
          voice_ports                                 8


Press [NextPage], [PrevPage] or [Cancel]
enter command: list configuration
```

3 Contact your Avaya representative if you need more than the enabled number of ports or if you want to add TCP/IP networking.

Change number of administered remote users

The number of administered remote users must be ≥ the number of mailboxes on every remote system networked with this local system.

To change the number of administered remote users:

1 Start at the AUDIX command prompt screen.

2 Enter **change system-parameters limits** at the `enter command` prompt.

The System-Parameters Limits screen displays:

```
                Active          Alarms: MmwA                 Logins: 3
change system-parameters limits                          Page 1 of 1
                        SYSTEM-PARAMETERS LIMITS

MESSAGE LIMITS
Message Lengths, Maximum  (seconds): 1200   Minimum  (tenths of seconds): 10
  Messages,  Total In All Mailboxes: 50000          Awaiting Delivery: 5000

ADMINISTRATION LIMITS
  Subscribers,  Local: 15000    Administered Remote: 1000
Lists,  Total Entries: 200000     Lists/Subscriber: 100   Recipients/List: 250

enter command: change system-parameters limits
```

3 Enter the number of remote users in the Administered Remote field.

4 Press F3 to save the information in the system database.

The cursor returns to the command line, and the system displays the following message:

`Command Successfully Completed`.

5 Enter **exit** or another administrative command.

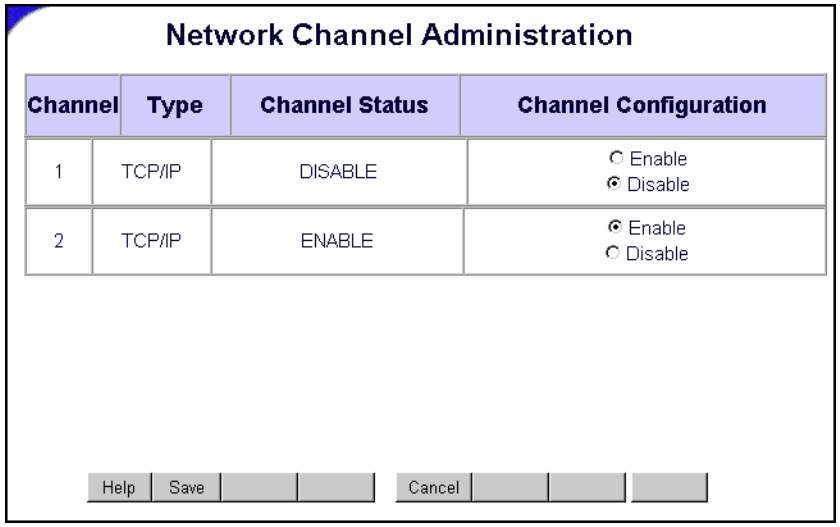
Administer networking channels

Enable the network channels so that the local AUDIX system can exchange voice messages over the digital network. Enabling the channels creates a communication link between the ACCX card and the switch or between the LAN card and the LAN and/or the wide area network (WAN).

To enable the network channels:

1 Start at the S8100 main page from Internet Explorer, and select **Administer System** → **AUDIX Networking** → **Administrative Menu** → **Network Channel Administration**.

The system displays the Network Channel Administration window:



2 Click **Enable** for each channel in the Channel Configuration column.

3 Click **Save**.

The system takes a few seconds to change the hardware configuration. The system displays a confirmation message when the process finishes.

Change local machine's information

You can change a local machine's information on its Machine Profile screen and on the Local Machine Administration window.

NOTE:
If you change a local machine's profile, inform every remote network administrator of the changes.

Change a local machine's profile

1. Start at the AUDIX command prompt screen.
2. Enter **change machine** at the `enter command:` prompt.

   The system displays the local machine's Machine Profile screen, page 1:

```
                    Active          Alarms: MmwA                  Logins: 2
change machine                                                    Page 1 of 2
                              MACHINE PROFILE

Machine Name: drmid10      Type: local          Location: local

 Voiced Name? n                                 Extension Length: 5
    Voice ID: 0                                Default Community: 1

ADDRESS RANGES
    Prefix                  Start Ext.   End Ext.        Warnings
 1: ____________________    36000        37999
 2: ____________________    _____        _____
 3: ____________________    _____        _____
 4: ____________________    _____        _____
 5: ____________________    _____        _____
 6: ____________________    _____        _____
 7: ____________________    _____        _____
 8: ____________________    _____        _____
 9: ____________________    _____        _____
10: ____________________    _____        _____

enter command: change machine
```

3. Complete the fields on this screen using the information from Table 29, Field definitions – page 1 of Machine Profile screen,, on page 213.

NOTE:
The Machine Name, Type, Location, Extension Length, and Voice ID fields are display only and cannot be changed except via the web page.

Table 29: Field definitions – page 1 of Machine Profile screen, *1 of 2*

Field	Valid input	Procedure/Description
Machine Name	Display only	Displays the local machine's Machine Name. This value comes from the network settings in Windows 2000.
Machine Type	Display only	Displays `local`.
Location	Display only	Displays `local`.
Voiced Name?	**y** = yes **n** = no	The Voiced Name field contains an **n** until you record a name for the machine. This field automatically changes to **y** when you record a name for the machine.
Extension Length	An integer, 3 – 10	Enter the length of extensions on the local system. The value you enter must match the extension length in your dial plan.
Voice ID	Display only	Displays a system-assigned identifier that you must use to identify the machine if you decide to record machine names.
Default Community	An integer, 1 – 15	If you have administered your system to use community sending restrictions, enter the default community number for your user population.
Prefix	0 – 21 alphanumeric characters	Prefixes can be used on the local machine, but they limit functionality and are not recommended. For details about the use and implications of prefixes, see the AUDIX Fax Administration documentation.

1 of 2

Table 29: Field definitions – page 1 of Machine Profile screen, *2 of 2*

Field	Valid input	Procedure/Description
Start Ext.	A 3- to 10-digit string	Enter the starting extensions for the ranges of telephone numbers used on the local system. (Designate a block of switch extensions that can be used at the local system when assigning users.) For example, if your system uses extensions between 2000 and 3000, enter **2000** in the Start Ext. field. Up to 10 different ranges can be specified to pinpoint the exact set of extension blocks used by the local system. The length of the start and end extension must agree with the Extension Length field. For a 5-digit extension, the default is 00000 to 99999.
End Ext.	A 3- to 10-digit string	Enter the ending extensions for the ranges of telephone numbers used on the local system. For example, if your system uses extensions between 2000 and 3000, enter **3000** in the End Ext. field.
Warnings	Display only	This field displays a warning when a duplication or overlap of an extension range for another machine is being assigned.

2 of 2

4 When you have finished entering information on this screen, press F7.

The system displays local machine's Machine Profile screen, page 2:

```
                    Active          Alarms: MmwA                Logins: 2
change machine                                                  Page 2 of 2
                              MACHINE PROFILE

Allow Automatic Full Updates? y

              Updates:    In? y        Out? y

          Network Turnaround? y

enter command: change machine
```

5 Complete the fields on this screen using the information provided in Table 30, Field definitions – page 2 of Machine Profile screen,, on page 215.

Table 30: Field definitions – page 2 of Machine Profile screen,

Field	Valid input	Description
Allow Automatic Full Updates	**y** = yes **n** = no	If **y**, the local AUDIX system automatically requests full updates from remote systems. If **n**, the local AUDIX system does not automatically request full updates from remote systems.
Updates: In?	**y** = yes **n** = no	If **y**, this local AUDIX system will accept updated user database information from any remote machine (the Updates In field must also be set to **y** on the remote Machine Profile screen setup on the local AUDIX system for each remote machine). If **n**, the local AUDIX system will not accept updates from any remote machine regardless of the entry on the remote Machine Profile screen. Set this field to **y** only after testing the network end-to-end during initial administration.
Updates: Out?	**y** = yes **n** = no	If you enter **y**, updates to user database information for local users are sent to a remote machine (the Updates Out field must also be set to **y** on the remote Machine Profile screen set up on the local AUDIX system for each remote machine). If you enter **n**, updates will not be sent to any remote machine regardless of the entry for this field on the remote Machine Profile screen. Set this field to **y** only after testing the network end-to-end during initial administration.
Network Turnaround	**y** = yes **n** = no	To disable this feature system-wide, enter **n** on the local Machine Profile screen. To enable the feature, enter **y** on the local Machine Profile screen *and* on the appropriate remote Machine Profile screens on this local system. If enabled, a network connection that originated from this local AUDIX system is allowed to turn around after the local AUDIX system has sent all of its network data to any remote machine. The remote machine may then return update information, voice mail, and status on the same connection.

6 When you finish updating the local machine's information, press **F3 [Enter]** to save the information in the system database.

The cursor returns to the command line, and the system displays the following message:

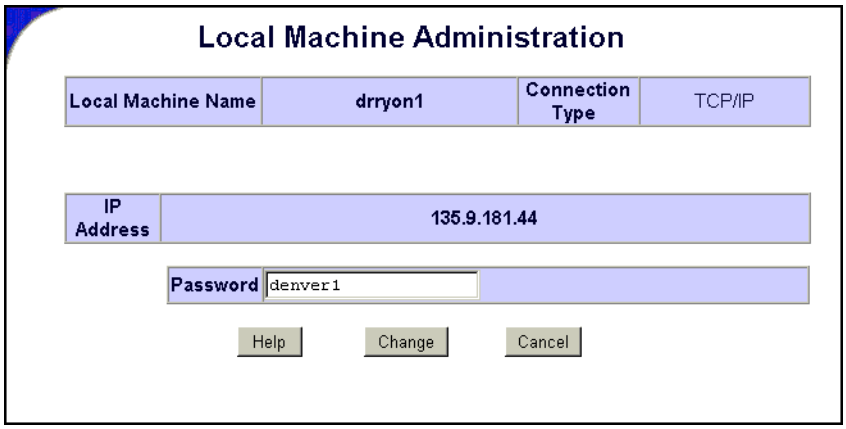
```
Command Successfully Completed.
```

7 Enter **exit** or another administrative command.

Complete the Local Machine Administration window

1 Start at the S8100 home page from the web browser, and select **Administer System** → **AUDIX Networking** → **Administrative Menu** → **Local Machine Administration**.

The Local Machine Administration window displays:



2 Change the password if necessary.

You cannot change the value in any fields except the Password field. To change other values, see Change a local machine's profile on page 212.

3 Click **Save**.

The system updates the information and displays a confirmation message.

Add a remote machine

If you want to enable users on the local machine to exchange messages with AUDIX users on another machine, you must provide information to the local machine about the remote machine.

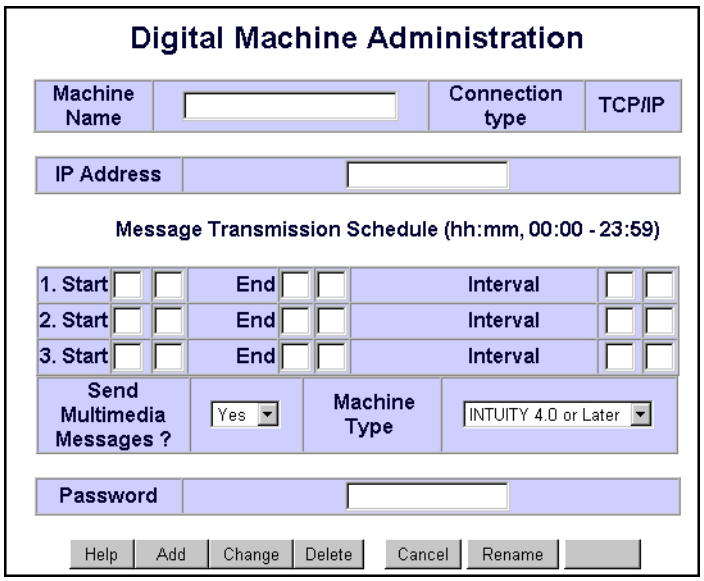
NOTE:
The AUDIX system accepts only 1 local machine. Do not attempt to add a second local machine. Use the instructions in this section only to add remote machines.

Complete the Digital Machine Administration window (via web browser)

To enter information for connecting to the remote machine:

1. Start at the S8100 home page, and select **Administer System** → **AUDIX Networking** → **Administrative Menu** → **Remote Machine Administration** → **Digital Machine Administration**.
2. On the Digital Machine Administration screen, click **Add New Machine**.

   The system displays the Digital Machine Administration window:



3. Complete the fields in this window using the information provided in Table 31, Field definitions – Digital Machine Administration window, on page 217.

Table 31: Field definitions – Digital Machine Administration window ***1 of 2***

Field	Valid input	Procedure/Description
Machine Name	1 – 10 alphanumeric characters; see guidelines at right	Enter the unique name of the remote machine. Each remote machine's name must be unique – not only to other remote machines, but to every machine on the network, including fax call delivery machines and the local AUDIX.
TCP/IP Address	Numeric address string in the format nnn.nnn.nnn.nnn	The IP address of the remote machine.

1 of 2

Table 31: Field definitions – Digital Machine Administration window ***2 of 2***

Field	Valid input	Procedure/Description
Message Transmission Schedule	24-hour clock time in the format *hh*:*mm*	`Start Time` – Enter the starting time for a message transmission period to the remote system, such as *00:01* for 1 minute after midnight. `End Time` – Enter the ending time for a message transmission period to the remote system, such as *23:59* for 1 minute before midnight. `Interval` – Enter the interval at which the local AUDIX system will call this remote system, such as *00:05* for every 5 minutes. The AUDIX system checks the queue at this interval and calls the remote system if something is in the queue for this remote system. Stagger start times and intervals for each remote system so the local AUDIX system does not try to call every remote system at the same time.
Password	5- to 10-digit alphanumeric characters	Enter the password exactly as it is administered on the remote system.
Send Multimedia Messages?	yes no	Select **yes** if the remote machine will accept multimedia messages (such as fax and text messages). Select **no** if the remote machine will not accept multimedia messages.
Machine Type	See description at right	Enter the machine type. To see a list of valid machine types, click the drop-down arrow and select the appropriate machine type from the available types.

2 of 2

4 When you finish entering information for a remote machine, click **Save**.

The system adds the information and displays a confirmation message.

5 Add another remote machine, if necessary.

Complete the Machine Profile screen for the remote machine (via AUDIX)

Use the Machine Profile screen to enter networking information required for each remote machine, such as address ranges and remote update information.

To enter networking information on the Machine Profile screen:

NOTE:
The Digital Machine Administration window must be completed for a remote machine before completing the Machine Profile screen for that machine.

1. Start at the AUDIX command prompt screen.
2. Enter **change machine *remote_machine_name*** at the `enter command:` prompt.

   The system displays the Machine Profile screen for a remote machine, page 1:

```
                    Active          Alarms: MmwA                    Logins: 2
change machine drbig10                                              Page 1 of 2
                              MACHINE PROFILE

Machine Name: drbig10      Type: VEX            Location: remote-digital

 Voiced Name? n                                 Extension Length: 5
    Voice ID: 1                                Default Community: 1

ADDRESS RANGES
    Prefix                  Start Ext.   End Ext.        Warnings
 1: _____                   53000        56999
 2: _____                   _____        _____
 3: _____                   _____        _____
 4: _____                   _____        _____
 5: _____                   _____        _____
 6: _____                   _____        _____
 7: _____                   _____        _____
 8: _____                   _____        _____
 9: _____                   _____        _____
10: _____                   _____        _____

enter command: change machine drbig10
```

NOTE:
If you do not know the names of the remote machines, enter **list machines** at the `enter command:` prompt. The system displays a list of every machine administered on the system.

3. Complete the fields in this window using the information provided in Table 32, Field definitions; remote machine profile screen, page 1,, on page 220.

NOTE:
The Machine Name, Type, Location, and Voice ID fields are display only and cannot be changed.

Table 32: Field definitions; remote machine profile screen, page 1, *1 of 2*

Field	Valid input	Description
Machine Name	Display only	Displays the machine name for this remote machine entered on the Digital Machine Administration window.
Type	Display only	Displays the machine type for this remote machine entered on the Digital Machine Administration window.
Location	Display only	Displays the location `remote-digital`.
Voiced Name?	**y** = yes **n** = no	The Voiced Name field contains an **n** until you record a name for the machine. This field automatically changes to **y** when you record a name for the machine.
Extension Length	An integer from 3 to 10	Enter the length of extensions on the local system. The value you enter must match the extension length in your dial plan.
Voice ID	Display only	Displays a system-assigned identifier that you must use to identify the machine if you decide to record machine names.
Default Community	An integer from 1 to 15	If you have administered your system to use community sending restrictions, enter the default community number for your user population.
Prefix	0 – 21 alphanumeric characters	Enter the prefix digits. A user enters the prefix before the remote user's extension when addressing voice messages. To simplify this task, use a short, descriptive prefix. The total length of the prefix plus the extension must not exceed 25 characters. The system uses the prefix only to identify users. It is not used for dialing out, so it does not need to match an area code or office code. The following are examples of possible prefixes: No prefix – The prefix is required only when one or more of the remote users share the same extension numbers as the local users (the extension ranges of the two systems overlap). If there are no overlapping extension numbers, a prefix is not needed. Public network access code – When addressing a message to a remote user, the local user enters the remote user's number as if placing a call to that user. Location code – This method simplifies addressing messages by requiring only an alphanumeric code in front of the extension number. Location codes are shorter and often easier to remember.

1 of 2

Table 32: Field definitions; remote machine profile screen, page 1, *2 of 2*

Field	Valid input	Description
Start Ext.	A 3- to10-digit string	Enter the starting extensions for the ranges of telephone numbers used on the local system. (Designate a block of switch extensions that can be used at the local system when assigning users.) For example, if your system uses extensions between 2000 and 3000, enter **2000** in the Start Ext. field. Up to 10 different ranges can be specified to pinpoint the exact set of extension blocks used by the local system. The length of the start and end extension must agree with the Extension Length field. For a 5-digit extension, the default is 00000 to 99999.
End Ext.	A 3- to10-digit string	Enter the ending extensions for the ranges of telephone numbers used on the local system. For example, if your system uses extensions between 2000 and 3000, enter **3000** in the End Ext. field.
Warnings	Display only	This field displays a warning when a duplication or overlap of an extension range for another machine is being assigned.

2 of 2

4 Press **F7 [NextPage].**

The system displays the Machine Profile screen for a remote machine, page 2:

```
                    Active          Alarms: MmwA                    Logins: 2
change machine drbig10                                              Page 2 of 2
                                MACHINE PROFILE

Send to Non-Administered Recipients? y

                      Updates:    In? y        Out? y

                  Network Turnaround? y

enter command: change machine drbig10
```

5 Complete the fields in this window using the information provided in Table 33, Field definitions; remote machine profile screen, page 2,, on page 222.

Table 33: Field definitions; remote machine profile screen, page 2,

Field	Valid Input	Description
Send to Non-Administered Recipients?	**y**= yes **n** = no	Enter **y** if the system will attempt to deliver messages to unadministered remote recipients. Enter **n** if messages cannot be sent to unadministered recipients.
Updates: In?	**y**= yes **n** = no	Enter **y** if the local system will accept updated database information from the remote system (the Updates Out field must also be set to **y** on the local Machine Profile screen). Set to **y** only after testing the network end-to-end during initial administration.
Updates: Out?	**y**= yes **n** = no	Enter **y** if the local system will send updated database information to the remote system (the Updates In field must also be set to **y** on the local Machine Profile screen). Set to **y** only after testing the network end-to-end during initial administration.
Network Turnaround	**y**= yes **n** = no	If you are conducting an acceptance test, enter **n**. After the acceptance tests, enter **y** if a network connection that originated from this remote system is allowed to turn around after the remote system has sent all of its network data to the local system. The local system may then return update information, voice mail, and status on the same connection. This feature reduces toll charges and increases the efficiency of the system in networks with more than 10 machines. The Network Turnaround field must be set to **y** on the local Machine Profile screen for this feature to work between the local system and the remote system.

6 Press **F3 [Enter]** to save the information.

The cursor returns to the command line, and the system displays the following message:

`Command Successfully Completed.`

7 Press **F3 [Cancel]** to return to the command line.

8 Enter **exit** or another administrative command at the `enter command:` prompt.

Perform a full remote update

If you have the system set to perform automatic daily updates, you only need to perform the full remote update to update the system after making changes to remote machine connections or to verify changes of data you just entered.

To update the remote user information immediately:

1. Start at the AUDIX command prompt screen.
2. Enter **get remote update *machine_name*** at the `enter command:` prompt, where machine_name is the name of the remote machine.

   The system displays the Remote Update Request confirmation screen.
3. Press **F3 [Enter]** to continue.

   The cursor returns to the command line, and the system displays the following message:

   `Command Successfully Completed`.
4. Enter **exit** or another administrative command at the `enter command:` prompt.

Reset automatic deletion of nonadministered remote users

To conserve server space by automatically deleting nonadministered remote users:

1. Start at the AUDIX command prompt screen.
2. Enter **change system-parameters features** at the `enter command:` prompt.

   The system displays the System-Parameters Features, page 1 screen.
3. Press F7 3 times to display the System-Parameters Features, Page 4 screen.
4. In the Days without Activity field, type the number of days. Type **0** if you do not want to automatically delete nonadministered remote subscribers.
5. In the Even If on a Mailing List? field, type **n** to retain information for nonadministered remote subscribers that are on a subscriber's mailing list.
6. Press F3 to save the changes.

   The cursor returns to the command line, and the system displays the following message:

   `Command Successfully Completed`.
7. Enter **exit** or another administrative command.

View remote extensions

To verify that the local machine database updated the remote subscriber information, view the remote extensions:

1. Start at the AUDIX command prompt screen.
2. Enter **list remote-extensions machine_name** at the `enter command:` prompt, where the machine_name is the local machine of the remote subscribers.

   The system displays the List Remote Extensions screen.
3. Press F7 to display additional pages of the list.
4. Press F1 to return the cursor to the command line.
5. Enter **exit** or another administrative command.

5 Upgrade and repair procedures

This chapter provides an overview of the procedures to upgrade and repair the S8100 system. See the Job Aid sections in Chapter , "Checklists and job aids" at the beginning of this document for the steps to perform the upgrade procedures. The repair procedures involving the replacement of the processor hard drive or circuit pack are the same as the corresponding upgrade procedures.

This chapter is organized as follows:

- Replace a TN795 Processor circuit pack on page 225
- Replace the TN2314 Processor circuit pack on page 226
- Replace the hard disk on page 226
- Download firmware to port circuit packs on page 227

Replace a TN795 Processor circuit pack

This section shows the basic steps to follow when replacing a TN795 circuit pack with a TN2314 circuit pack. The TN2314 replaced the TN795 with release 10. These steps assume the technician will connect a laptop directly to the Service Access jack on the faceplate of the TN2314.

Inventory existing features on the pre-R10 switch and obtain a license file

If the valid license file does not already exist on the system or your laptop, the license file must be obtained using Remote Feature Activation (RFA). If you are an approved RFA user, you can obtain and install the license file. To become an approved RFA user, you must attend RFA training.

Before obtaining a new license file, you must inventory the existing features and capacities of the TN795 using the Feature Extraction tool (FET). The FET must be downloaded to your PC by going to one of the Remote Feature Activation (RFA) web sites indicated in Go to the RFA web site on page 166. FET will provide you with an encrypted switch-configuration file that must be used on the RFA web site to create a license file.

See License file, password file, and installation script overview on page 164 for information about obtaining and installing license files.

NOTE:
With Release 10 and later, the *init* (lucent1) login no longer has the capability to change the customer options, offer option, or special applications forms.

Replacing a TN795 with a TN2314

NOTE:
If you have any additional login accounts and passwords or software that is not Communication Manager loaded on the system, you will have to reconstruct or reload this information on the new TN2314 or it will be lost. Write down any information you need from the old system that will enable you to add it to the new system.

Follow the steps in the Job Aid, Upgrade an S8100's R9.5 software by replacing the S8100 on page 26 to replace the TN795 with the TN2314 Processor circuit pack.

Replace the TN2314 Processor circuit pack

This section outlines the procedures to replace an existing TN2314 Processor circuit pack.

NOTE:
If the TN2314 circuit pack is replaced for repair, a new license file must be obtained and installed. Communication Manager, INTUITY AUDIX, and SNMP will not start if the license file does not match the new TN2314's serial number. Ensure that the new circuit pack has solved the problem before you access RFA to update the license file.

See License file, password file, and installation script overview on page 164 and subsequent sections, for information about obtaining and installing license, password (authentication), and installation-script files.

NOTE:
When you swap out a processor that has an RFA-generated license file, the faulty processor must be returned to repair. It is not re-usable because the serial number of the swapped out processor has been captured within an SAP database and is marked as unusable. If you try to generate a license against it, you will be denied.

To replace a TN2314 circuit pack, follow the steps in the Job Aid, Upgrade an S8100's R9.5 software by replacing the S8100 on page 26, and substitute "new TN2314" for "TN795."

Replace the hard disk

The hard disk on the TN2314 Processor circuit pack will need to be replaced if it is defective or needs to be upgraded. To replace the hard disk, follow the steps in the Job Aid, Replace an S8100's hard drive on page 20.

Download firmware to port circuit packs

You can download updated application code for a port circuit pack on site or remotely. This eliminates the need to physically remove the circuit pack and send it to the factory for the firmware update.

The port circuit packs supported are:

- UDS1 – TN464GP, TN2464BP, and TN2313AP
- DIG-LINE – TN2214CP and TN2224CP
- Maintenance/Test – TN771DP
- IP Media Processor – TN2302AP
- Voice Announcement over LAN (VAL) – TN2501AP
- C-LAN – TN799DP

The P suffix designation means the circuit pack is programmable; new firmware can be downloaded directly to the circuit pack.

See the FW-DWNLD maintenance object in *Maintenance for the Avaya S8100 Media Server with the Avaya G600 and the Avaya CMC1 Media Gateways*, 555-233-149, for detailed instructions on downloading firmware. This information is also available on the Avaya Support web site, http://www.avaya.com/support.

6 Hardware additions

This chapter provides the tasks required to install equipment associated with upgrading an existing S8100 system.

For more information about installing adjuncts and peripheral devices, see *Installation for Adjuncts and Peripherals for Avaya Communication Manager* (555-233-116).

This chapter is organized as follows:

- Add circuit packs on page 229
- Add IP trunk on page 230
- Add remote office on page 230
- Add C-LAN functionality on page 230
- Add TN464GP/TN2464BP with echo cancellation on page 234
- Add CO, FX, WATS, and PCOL on page 236
- Add DID trunks on page 236
- Add Tie trunks on page 237
- Add DS1 tie and OPS on page 238
- Add speech synthesis on page 239
- Add Code Calling access on page 239
- Multiple integrated recorded announcements on page 239
- Add ISDN-PRI on page 242
- DEFINITY LAN gateway (DLG) on page 243

Add circuit packs

When installing additional features or equipment, it may be necessary to install additional circuit packs. For a list of allowed circuit packs, see Allowed circuit packs and circuit modules on page 86. This is a general procedure to use when adding features or equipment that require adding circuit packs.

1. Log into the system, and answer **y** to the *Suppress Alarm Origination* question during login.
2. Install the circuit pack in the carrier.
3. Type **change circuit-pack**.
4. Verify that the circuit pack appears in the listing.
5. If the circuit pack code does not appear, type the code manually in the proper slot.
6. Type **test board long** command to test the circuit pack.
7. Log off the system after the addition (and any required administration) is complete.

For information about administering circuit packs and other equipment, see the *Administrator's Guide for Avaya Communication Manager* (555-233-506).

Add IP trunk

For IP Media Processor set up instructions, refer to *Administration for Network Connectivity for Avaya Communication Manager* (555-233-504).

Add remote office

S8100 can connect to the Avaya R300 Remote Office Communicator (Avaya R300) in a remote office configuration. Avaya R300 operates like a simple switch at the remote site for connections made between remote stations, as well as between remote stations and local access trunks. It receives incoming PSTN dialed data calls and terminates them on the correct data modem.

Using a standard 25-pair cable, you can connect Avaya R300 to a 110 punch-down wall field. Avaya R300 connects to a set of harmonica adapters by way of a cable that adapts between the connection on the circuit pack and the harmonica adapter and uses phantom power to power every analog and DCP telephone.

For information about installing and administering Avaya R300 Communicator, see *Getting Started with the Avaya R300 Remote Office* (555-233-769) and *MAX 3000 Installation and Basic Configuration Guide* (555-233-768).

Add C-LAN functionality

IP Softphone is available with S8100. In addition, corresident C-LAN functionality can be optionally purchased. The S8100 WIndows 2000 LAN interface may be used in place of the C-LAN circuit pack for those cases where DS1 capability through the C-LAN is not required. DCS using DS1 will still be supported via a separate C-LAN. The Windows LAN interface (corresident C-LAN) will also be used to connect CMS, BCMS Vu, and CentreVu-CT. See the *Overview for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways* (555-233-231).

Add a TN799DP C-LAN circuit pack

NOTE:
The TN799DP version of C-LAN is required for the use of IP Softphones.

To add a TN799DP C-LAN circuit pack, complete the following procedures:

- Install the TN799DP
- Test the External Connection to the LAN
- Administer the TN799DP on the SAT

Install the TN799DP

To install a TN799DP C-LAN circuit pack, you need the following items:

- An unoccupied port slot
- A 10 BaseT Ethernet connection into your local area network
- A valid, unused IP addresses on your network for each C-LAN circuit pack

CAUTION:
When adding or replacing any hardware, be sure to ground yourself against electrostatic discharge (ESD) by wearing a grounded wrist strap.

NOTE:
The TN799DP circuit pack is hot-swappable, so you do not need to power down the carrier to install it.

From the rear of the cabinet:

1. Connect the 259A connector to the backplane connector corresponding to the TN799DP slot.
2. Connect one end of the CAT5 cable to the 259A connector. Connect the other end to the customer's network.

From the front of the cabinet:

1. Insert the TN799DP circuit pack into the port slot identified earlier.

Administer the TN799DP on the SAT

1. Type **change node-names ip** and press Enter.

```
 change node-names ip                                          Page   1 of
1
                                  NODE NAMES

    Name              IP Address           Name              IP Address
clan2               135.9  .167.179                            .   .   .
default             0  .0  .0  .0                              .   .   .
clan1               192.168.10 .21                             .   .   .
                       .   .   .                               .   .   .
                       .   .   .                               .   .   .
                       .   .   .                               .   .   .
                       .   .   .                               .   .   .
                       .   .   .                               .   .   .
                       .   .   .                               .   .   .
                       .   .   .                               .   .   .
                       .   .   .                               .   .   .
                       .   .   .                               .   .   .
```

2. In the Name and IP Address fields, type a name and IP address for each PC that will be *dialing into* the C-LAN circuit pack; up to 8.

3 Type **change ip-interfaces** and press Enter.

```
change ip-interfaces                                        Page   1 of   4

                                  IP INTERFACES
 Inter-region IP connectivity allowed?  n
Enable                                                                  Net
Eth Pt Type   Slot  Code Sfx Node Name      Subnet Mask     Gateway Address Rgn
   n   C-LAN  01A09 TN799  B clan-a1       255.255.255.0   192.168.10 .21   1
   n   C-LAN  01B03 TN799  B ppp10         255.255.255.0   135.9  .167.179  1
   n                                       255.255.255.0      .   .   .
   n                                       255.255.255.0      .   .   .
   n                                       255.255.255.0      .   .   .
   n                                       255.255.255.0      .   .   .
   n                                       255.255.255.0      .   .   .
   n                                       255.255.255.0      .   .   .
   n                                       255.255.255.0      .   .   .
   n                                       255.255.255.0      .   .   .
   n                                       255.255.255.0      .   .   .
   n                                       255.255.255.0      .   .   .
```

NOTE:
Do not change the Enabled field to **y** until all of the information in the row is completed.

4 Fill in a row for each TN799DP circuit pack installed.

Use the same node name assigned on the Node Names screen. You can press Help in the Node Name field to display every valid node name. Use the gateway address for the *router* connected to the hub; *not* the hub.

5 Type **y** in the Enabled field for each completed row.

6 Type **change IP services** and press Enter.

Do not change the Enabled field to **y** until all of the information in the row is completed.

7 Fill in the following fields:

- Service Type: xxx
- Local Node: slot location of the TN799DP
- Local Port: any open port, generally 9001 or higher
- Remote Node: a specific PC node name assigned on the IP Interfaces screen. Do not type **any**
- Remote Port: xxx

8 Type **y** in the Enabled field for each completed row. Enabling the local node turns on the listen socket.

Test the external connection to the LAN

To test the external IP connections, ping the C-LAN server and ping a known computer connected to your network. If everything is configured correctly, the **Result** column on the Ping Results screen reads **pass**. If it reads **abort**, verify the IP-address information and check the connectivity, including the cabling.

1 Type **ping ip-address *nnn.nnn.nnn.nnn* board *UUCSS*** and press Enter. The variable ***nnn.nnn.nnn.nnn*** is the IP address of the TN799DP C-LAN circuit pack and ***UUCSS*** is the cabinet, carrier, and slot of the TN799DP C-LAN circuit pack.

```
ping ip-address 192.168.10.21

                          PING RESULTS

  End-pt IP        Port      Port Type  Result    Time(ms)  Error Code

  192.168.10.21    01A13      CLAN      PASS       10        1124
```

2 Type **ping ip-address *nnn.nnn.nnn.nnn* board *UUCSS*** and press Enter. The variable ***nnn.nnn.nnn.nnn*** is the IP address of the customer's gateway and ***UUCSS*** is the cabinet, carrier, and slot of the TN799DP C-LAN circuit pack.

3 Type **ping ip-address *nnn.nnn.nnn.nnn* board *UUCSS*** and press Enter. The variable ***nnn.nnn.nnn.nnn*** is the IP address of another computer beyond the gateway and ***UUCSS*** is the cabinet, carrier, and slot of the TN799DP C-LAN circuit pack.

The TN799DP C-LAN circuit pack is now installed in the G600/CMC1 carrier and connected to the IP network.

Communication Manger

Avaya offers several IP solutions for customers, 2 of which are Avaya R300 Remote Office Communicator and the IP Media Processor. For information about the Avaya R300, refer to *Getting Started with the Avaya R300 Remote Office* (555-233-769) and *MAX 3000 Installation and Basic Configuration Guide* (555-233-768).

Communication Manager operates both as an IP gateway and gatekeeper. As a gateway it converts voice traffic to data transmission over IP networks. As a gatekeeper, it provides IP endpoints with secure access to the S8100/G600/CMC1 system. This connection lets users take advantage of every application on the system, including voice mail, computer-telephone integration, call center, wireless, and call control features, such as conferencing, call forward, transfer, hold, speed-dial, and multiple-line appearances.

The software supports Distributed Communications System DCS and Q-Signaling (QSIG) protocols over IP networks to operations across multiple sites. Communication Manager can be managed through the server's existing system-administration tools, and can take advantage of call routing and cost accounting, self diagnostics, toll-fraud security protection, and remote access applications. It enables IP telephones to communicate with analog, digital, and ISDN phones on the network, and supports the H.323 protocols and standard application programming interfaces, including TAPI, TSAPI, and JTAPI.

Several new corresident applications free up slots in the cabinet, including C-LAN functionality, announcements, and DEFINITY LAN Gateway. In most cases, with these applications corresident, separate C-LAN and Announcement circuit packs are not required and MAP-D is not required for DEFINITY LAN Gateway. Also BCMS Vu and CentreVu-CT reside on a separate server, which is LAN connected and enables S8100 to interface with these applications.

NOTE:
The C-LAN (TN799DP) is still required for IP phones. C-LAN can be used instead of, or in addition to, the processor Ethernet interface for DEFINITY LAN Gateway connectivity.

Add TN464GP/TN2464BP with echo cancellation

The TN464GP and TN2464BP circuit packs with echo cancellation are intended for S8100/G600/CMC1 customers who are likely to encounter echo over circuits connected to the Direct Distance Dialing (DDD) network. These circuit packs are intended for channels supporting voice; therefore, they support the following trunks: CAS, CO, DID, DIOD, DMI, FX, Tie, WATS. They do not support any data trunk groups.

NOTE:
The P suffix designation means the circuit pack is programmable; new firmware can be downloaded directly to the circuit pack.

The TN464GP and TN2464BP circuit packs are backward compatible, although the echo-cancellation feature can only be used with Release 9 or later software and after the feature is enabled.

The echo-cancellation feature cancels echoes with delays of up to 96 ms. Echo cancellation is disabled automatically when the circuit pack detects a 2100-Hz *phase-reversed* tone put out by a high-speed (56-kbps) modem, but not when it detects a 2100-Hz straight tone generated by a low-speed (9.6-kbps) modem .

For information about installing port circuit packs, refer to Installing Port Circuit Packs. For information about setting the option switches, refer to Option Switch Settings. For information about administering the circuit packs, refer to the *Administrators Guide for Avaya Communication Manager* (555-233-506).

Echo cancellation must first be purchased, then activated by someone with customer options login privileges. Refer to the *Administrators Guide for Avaya Communication Manager* (555-233-506).

Use the following procedure to modify the settings:

NOTE:
You do not need to busyout the circuit packs to modify the settings. But the modified settings do not take effect until either the port is busied out or the scheduled maintenance runs.

1 Type **display system-parameters customer-options**, and press Enter. On screen 2 verify that the `DS1 EchoCancellation?` field is set to **y**. If not, contact someone in your area with customer options login privileges.

2 Type **[add | change] trunk-group [next | number]** and press Enter.

```
add trunk-group next                                Page   2 of 11   SPE A
                          TRUNK FEATURES

             ACA Assignment? n                        Measured: both
             Internal Alert? n                Maintenance Tests? y
           Data Restriction? n
             Glare Handling: none

               Used for DCS? n
      Suppress # Outpulsing? n
Seize When Maintenance Busy: neither-end



Incoming Tone (DTMF) ANI: no            Per Call CPN Blocking Code:
         Connected to CO? n           Per Call CPN Unblocking Code:

                                          Ds1 Echo Cancellation? y
```

3 On Trunk Features, screen 2, set the DS1 Echo Cancellation? field to **y**.

4 Type **[add | change] ds1 *UUCSS*** and press Enter.

```
add ds1 2b08                                      Page   1 of 1   SPE B

                                 DS1 CIRCUIT PACK

             Location: 02B08                        Name: Echo Cancel t23
             Bit Rate: 2.048                Line Coding: hdb3

       Signaling Mode: CAS

         Interconnect: pbx             Country Protocol: 1

Interface Companding: mulaw                         CRC? n
           Idle Code: 11111111



       Slip Detection? y              Near-end CSU Type: other

   Echo Cancellation? y
        EC Direction: inward
    EC Configuration: 1
```

5 On the DS1 Circuit Pack screen, set the Echo Cancellation? field to **y**.

When set to y, 2 new fields display: EC Direction: and EC Configuration:

- If you know the echo is coming into S8100/G600/CMC1, keep the default setting for the EC Direction: field of **inward**.
- If you know that the distant party is hearing echo that originates in S8100/G600/CMC1 or its line side stations or equipment, set the EC Direction: field to **outward**.

Keep the default setting for the EC Configuration: field of **1**. This setting rapidly minimizes echo when first detected, regardless of the volume of the talker's voice.

6 Test the voice quality on a telephone connected through the TN464GP or TN2464BP circuit packs and known to have echo to see if the echo was eliminated.

7 If the echo still exists, set the `EC Configuration:` field to **2**, **3**, or **4**, then test the voice quality. These settings provide help for the following scenarios:

- Setting 2 – Minimizes speech clipping, but it takes a fraction of a second longer for the echo to fade.
- Setting 3 – Eliminates speech clipping, but a strong echo may take 2 or 3 seconds to fade.
- Setting 4 – Minimizes extremely strong echo, very hot signals, or excessive clipping or breakup of speech from a distant party. It reduces speech clipping but may allow slight residual echo or more background noise.

8 If the echo still exists after trying every previous setting, contact technical support.

Add CO, FX, WATS, and PCOL

Requirements

Each Central Office (CO), Foreign Exchange (FX), Personal Central Office Line (PCOL), or Wide Area Telecommunications Service (WATS) trunk connects to 1 port of either an 8-port TN747B or to 1 of several CO trunk circuit packs.

Installation

1 Determine the port assignment of the trunk from Trunk Group form.

EXAMPLE:	Port number	3	A	07	01
		Cabinet	Carrier	Slot	Circuit
		(Port network)	(or compact modular cabinet)		

2 Install a TN747B or a CO Trunk circuit pack in the assigned carrier slot (if an additional circuit pack is required).

3 Administer the forms listed under CO, FX, WATS, or PCOL Trunk Group in *Administrator's Guide for Avaya Communication Manager* (555-233-506).

Add DID trunks

Requirements

Each Direct Inward Dial (DID) trunk connects to 1 port DID Trunk circuit pack or to 1 port of an assortment of DID trunk circuit packs.

Installation

1 Determine the port assignment of the trunk from Trunk Group form.

EXAMPLE:	Port number	1	A	07	01
		Cabinet	Carrier	Slot	Circuit
		(Port network)	(or compact modular cabinet)		

2 Install a DID Trunk circuit pack in assigned carrier slot (if an additional circuit pack is required).

3 Administer forms listed under “DID Trunk Group” in *Administrator’s Guide for Avaya Communication Manager* (555-233-506).

Add Tie trunks

Requirements

Each tie trunk connects to 1 port of a 4-port Tie Trunk circuit pack or to an assortment of international Tie Trunk circuit packs.

Installation

1 Determine the port assignment of the trunk from Trunk Group form.

EXAMPLE:	Port number	3	A	02	01
		Cabinet	Carrier	Slot	Circuit
		(Port network)	(or compact modular cabinet)		

2 Install a Tie Trunk or an international Tie Trunk circuit pack in assigned carrier slot (if an additional circuit pack is required).

3 For customer-owned (not leased) tie-trunk facilities (such as campus environments), Tie Trunk circuit packs provide signaling capabilities beyond those specified by the industry-wide E&M standard. Use Figure 48, Tie Trunk circuit packs (component side), on page 238 and Table 34, Tie trunk option-switch settings and administration, on page 238 to choose the preferred signaling format, set switches on the circuit pack, and administer the port.

4 Administer forms listed under “Tie Trunk Group” in the *Administrator’s Guide for Avaya Communication Manager* (555-233-506).

Figure 48: Tie Trunk circuit packs (component side)

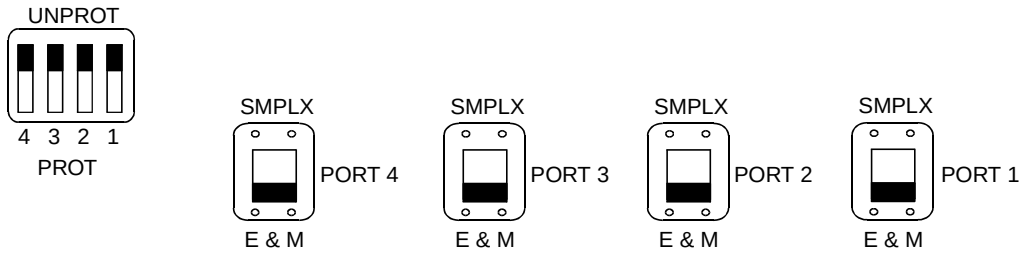


Table 34: Tie trunk option-switch settings and administration

Installation situation		Preferred signaling format		E&M/SMPLX switch	Prot/Unprot switch	Administered port
Circumstance	**To**	**System**	**Far-End**			
Collocated	Communication Manager	E&M Type 1 Compatible	E&M Type 1 Standard	E&M	Unprotected	Type 1 Compatible
Inter-Building	Communication Manager	Protected Type 1 Compatible	Protected Type 1 Standard Plus Protection Unit	E&M	Protected	Type 1 Compatible
Collocated	Net Integrated	E&M Type 1 Standard	Any PBX	E&M	Unprotected	Type 1

Add DS1 tie and OPS

Service interruption

Because the addition of DS1 tie-trunk service may require a service interruption, notify the customer when the addition will occur.

Add speech synthesis

The TN725B Speech Synthesizer circuit pack is required when Voice Message Retrieval, Automatic Wakeup, or Do Not Disturb features are activated. The TN725B circuit pack does not require administration.

1. Determine the port assignment of the Speech Synthesizer circuit pack being added.
2. Install the TN725B Speech Synthesizer circuit pack in the designated carrier slot.

Add Code Calling access

The tones for the Code Calling feature are generated by the TN2182/B tone-clock circuit pack in the port networks.

1. Install a TN763B/C/D auxiliary trunk circuit pack or a TN457 speech synthesizer circuit pack and connect for Loudspeaker Paging. The Code Calling Access feature shares the same ports as Loudspeaker Paging. An auxiliary trunk circuit pack provides 4 ports for Loudspeaker Paging and Code Calling Access.
2. Administer the form listed under “Code Calling Access” in *Administrator’s Guide for Avaya Communication Manager* (555-233-506).

Multiple integrated recorded announcements

S8100 provides 3 methods of integrated announcements. Both can be used on the same system. The methods are:

- TN750C Announcement circuit pack
- CWY1 announcements
- TN2501 VAL circuit pack

NOTE:
The .wav files that contain an S8100’s announcements can be used with the VAL (voice announcements on the LAN) circuit pack in other DEFINITY server systems ***only if*** the S8100’s .wav-file attributes match those used by VAL. To use an S8100’s .wav files with VAL, they must be created with the following attributes – PCM-encoded, 8 bits per sample, 8-kHz sampling rate, and single-channel (Mono) mode.

TN750C Announcement circuit pack

The TN750C circuit pack contains on-board flash memory that provides internal backup of announcements. Thus, the TN750C circuit pack does not require the save and restore processes. TN750C announcements cannot be backed up and restored to an external device with an S8100 system.

The TN750C circuit pack can replace a TN750 or TN750B. The difference in operation is that the TN750C automatically restores and reports the availability of announcements from its internal flash memory in 5 minutes, rather than the 40 minutes for the TN750 or TN750B.

If a circuit pack already has announcements in its flash memory, the yellow LED flashes as the announcements copy to the voice RAM.

Add TN750C circuit pack

Follow this procedure to add a circuit pack:

1. Insert the TN750C into a vacant slot in a carrier.
2. Administer new announcements to the TN750C's slot by executing the **change announcements** <**location**> command.
3. Record the announcements, as described in *Administrator's Guide for Avaya Communication Manager* (555-233-506).
4. Wait until the announcements copy from voice RAM to the on-board flash memory (the yellow LED on the TN750C starts and then stops flashing). This takes about 10 minutes.

Move a single announcement to another Announcement circuit pack

Follow this procedure to move a single announcement to another Announcement circuit pack:

1. Enter the **change announcements** command to change the circuit pack locations of a particular announcement. (You may also change the compression rate at this time.)
2. Re-record the announcement, as described in *Administrator's Guide for Avaya Communication Manager* (555-233-506).

CWY1 announcements

With CWY1 announcements, customers can produce and use professional quality announcements and store them on the S8100 hard drive. Voice processing of the announcements is handled on the CWY1 board. The CWY1 board is resident as a component of the TN2314 Processor circuit pack. Handling announcements on the CWY1 board eliminates the need for the TN750 circuit pack, thus freeing the slot occupied by the TN750 circuit pack. CWY1 announcements can be stored on the S8100 hard drive and backed up and restored to a LAN drive.

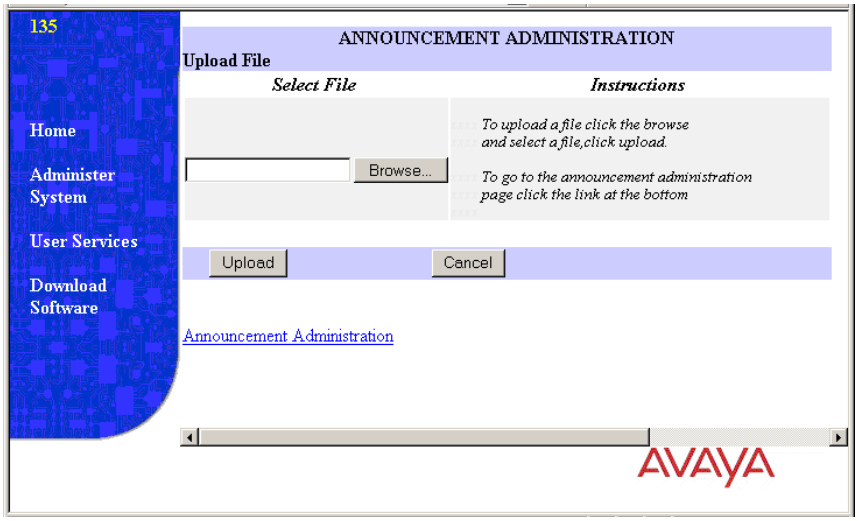
To install CWY1 announcements, you use the S8100 user interface to upload the announcements file from a server directory to the announcements directory. The file is moved to the appropriate announcements directory and converted from WAV format to speech format.

CWY1 announcements can also be recorded in the same manner as the TN750C. The virtual port location is 1A13 for CWY!.

Installing CWY1 announcements

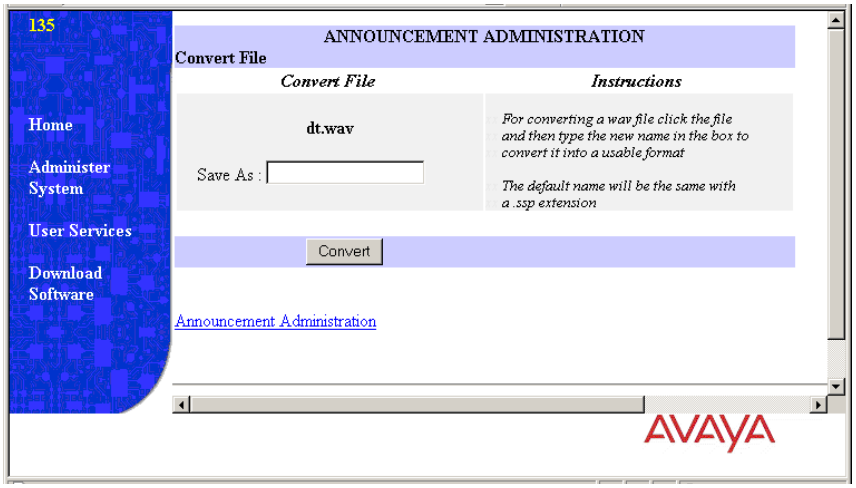
To install CWY1 announcements:

1. From the S8100 home page, click **Administer System**. The **System Administration** page displays.
2. Click **Announcement Admin.** The **Announcements Administration** page displays.
3. Click **Upload File**. The **Upload File** page displays:



4. Enter the name of the announcements file that you want to upload and click the **Upload** button. After the file is uploaded, a message box displays and asks whether you want to convert the file.
5. Choose **Yes.**

   The **Convert File** page displays:



6. Enter a name for the converted file and click **Convert.** The announcements file is converted to speech format and saved in the announcements directory.

   See *Administrator's Guide for Avaya Communication Manager* (555-233-506) for information about administering CWY1 announcements.

Add ISDN-PRI

T1 (North American standard)

This procedure describes adding a T1 line.

1. Use a TN767F or TN767E (or later version) circuit pack to set up an ISDN PRI trunk. Ensure that the dip switch on the circuit pack is set for 24 channels. If you are using Facility Associated Signaling (FAS), 23 channels are available to be used as trunk group members. Channel 24 must be used to create a signaling group for the trunk groups. If you are using Non Facility Associated Signaling (NFAS), it is possible, in some instances, to use all 24 channels for trunk group members.
2. To create a PRI trunk:
   a. Enter **ADD DS1** (circuit pack location) at the SAT terminal session.
   b. Enter the required information on the DS1 form.
   c. Create a signaling group using the **ADD SIG NEXT** command. If you are using FAS signaling, use the 24th channel on your DS1 circuit pack as the D channel for your signaling group. If you are using NFAS signaling, enter **N** in the associated signaling field. List the trunk circuit pack location in the Trunk Board field.
   d. Create a trunk group by using the **ADD TRUNK NEXT** command:
      1. Complete the required information on the Trunk Group form's pages.
      2. Enter the port locations of the trunk members on the Trunk Group Member page.
      3. Enter the correct signaling group number.

E1 (international standard)

1. Use a TN464F circuit pack. Ensure that the dip switch on the circuit pack is set for 30 channels (E-1). If you are using Facility Associated Signaling (FAS), 29 channels are available to be used as trunk group members. Channel 16 must be used to create a signaling group for the trunk groups. If you are using Non Facility Associated Signaling (NFAS), it is possible to use all 30 channels for trunk group members in some instances.
2. To create a trunk group, do the following:
   a. Determine the slot assignment of the circuit packs to be added.
   b. Install the DS1 Interface circuit pack in the assigned carrier slot.
   c. Enter **ADD DS1** (circuit pack location) at the SAT terminal session.
   d. Enter the required information on the DS1 form.
   e. Create a signaling group using the **ADD SIG NEXT** command. If you are using FAS signaling, use the 16th channel on your DS1 circuit pack as the D channel for your signaling group. If you are using NFAS signaling, enter **N** in the associated signaling field. List the trunk circuit pack location in the Trunk Board field.
   f. Create a trunk group by using the **ADD TRUNK NEXT** command:
      1. Complete the required information on the Trunk Group form's pages.
      2. Enter the port locations of the trunk members on the Trunk Group Member page.
      3. Enter the correct signaling group number.

Add circuit packs

1. Determine the slot assignment of the circuit packs to be added.
2. Install the DS1 Interface circuit pack in the assigned carrier slot.

Install cables

Install cables from the cabinet to the MDF as required.

Enter added translations

1. Administer the forms listed under “Integrated Services Digital Network – Primary Rate Interface” in *Administrator’s Guide for Avaya Communication Manager* (555-233-506).

Resolve alarms

1. Examine the alarm log. Resolve any alarms that may exist using *Maintenance for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Gateway Medias* (555-233-149).

Save translations

1. Enter **save translation**, and press Enter. This instructs the system to take all translation information in memory and write it to the translation cards.
2. Update backup cards, if necessary.

DEFINITY LAN gateway (DLG)

The S8100 system supports both the external MAP-D and corresident implementations of DEFINITY LAN Gateway (DLG).

The corresident DEFINITY LAN Gateway (DLG) provides CTI link connectivity for ASAI to ASAI adjuncts, including CentreVu- CT. Connectivity is provided between S8100 and an ASAI adjunct using the IP interface on the TN2314 circuit pack and/or the C-LAN TN799 circuit pack. Multiple CTI links are supported. Up to 8 links can be administered.

For more information about DLG, see:

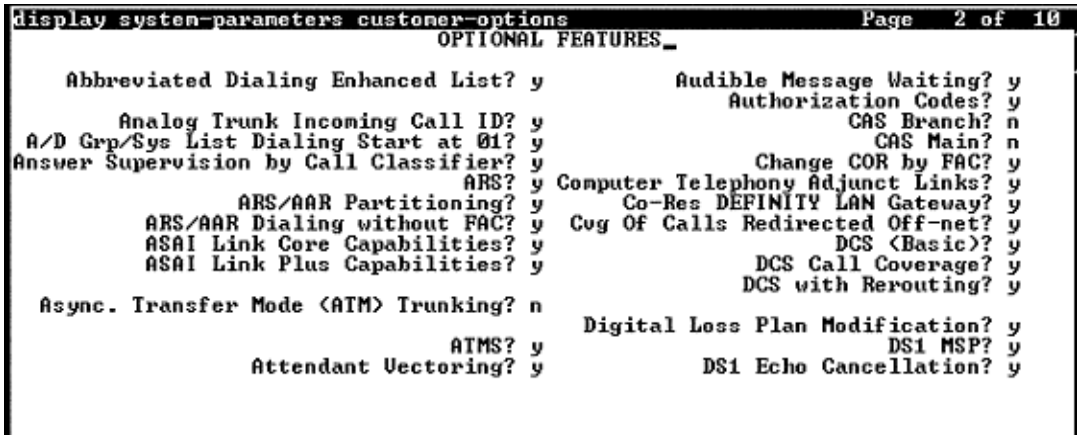
- *Administrator’s Guide for Avaya Communication Manager*, 555-233-506.
- *CallVisor ASAI Technical Reference*, 555-230-220.

Coresident DLG

The coresident DLG functionality is on the S8100 Media Processor. This feature must be enabled in the license file. If so, the Co-Res DEFINITY LAN Gateway? field on the System-Parameters Customer-Options form will be set to **y**.

ADJ-IP and ASAI-IP are the two CTI link types supported by the coresident DEFINITY LAN Gateway (DLG) feature. The ASAI-IP link is the Adjunct Switch Application Interface (ASAI) link between S8100 and an ASAI adjunct. The Adjunct IP link is the ASAI proprietary link between S8100 and CentreVu-CT. The ASAI endpoint is connected to an Ethernet LAN.

To use the ASAI-IP and ADJ-IP link types, the license file must turn on the following features: “Co-Res DEFINITY LAN Gateway” *and* “ASAI Link Core Capabilities” (for ASAI-IP links) and/or “Computer Telephony Adjunct Links” (for ADJ-IP links). These settings can be verified by displaying the System-Parameters Customer-Options form. In addition, the links must be administered on the DLG Administration page of the IP Services form.



7 Avaya Site Administration

This chapter provides information about Avaya Site Administration, a system-management tool that the customer can purchase as an option with the Avaya Integrated Management Suite.

> **NOTE:**
> Although separately available to facilitate management of an S8100, Avaya Site Administration is ***not*** included as part of the S8100's standard software package.

For information about installing Avaya Site Administration, see Download Avaya Site Administration on page 197.

This chapter is organized as follows:

- Avaya Site Administration overview on page 245
- Interactions with switches and voice-mail systems on page 248
- Components of Avaya Site Administration on page 249
- How Avaya Site Administration works on page 251
- Avaya Site Administration help on page 251
- Install Avaya Site Administration on page 252
- Configure Avaya Site Administration on page 253
  - Add an S8100 switch-administration item on page 253
  - Add S8100 voice-mail administration item on page 254

Avaya Site Administration overview

Avaya Site Administration is a general-purpose system-management tool that simplifies basic administration of S8100 systems (with a G600 or CMC1 Media Gateway) and INTUITY AUDIX systems. Avaya Site Administration versions 1.0 and greater provide:

- A graphically enhanced command-line interface (called the Graphically Enhanced DEFINITY Interface, or GEDI) and a terminal emulation mode for SAT administration.
- Easy-to-use software with a Windows look and feel. The browser contains tabbed windows, menus, and dockable windows. The browser provides a tree view of the switches, voice-mail systems, commands, and tasks you can administer with Avaya Site Administration, as well as icons for accessing task wizards.
- Button Label Printing (BLP) for producing station labels for users' phones. You can print custom button labels on any laser printer and can preview each label before printing.
- Schedule Viewer, used for scheduling tasks and monitoring their progress. You can schedule a command to execute at any time in the future.
- History Log, which provides a history of events that Avaya Site Administration has initiated. The History tab displays feedback from a switch or voice-mail system about tasks that Avaya Site Administration has run, or attempted to run. The History Tab helps users identify and correct errors.

- Four modes of operation:
  - Task shortcuts, which provide tree-based access to Communication Manager switch commands, letting you quickly and easily find the necessary commands for command administration activities. Avaya Site Administration command folders include:
    - Abbreviated Dialing
    - Call Center
    - Coverage
    - Groups
    - Network
    - Parameters
    - Station
    - Status
    - System
- Task wizards, which provide shortcuts to common switch and voice-mail administration activities via an intuitive point-and-click interface, to help you quickly and easily perform the task. These wizards include:
  - Add Bridged Appearance
  - Add User
  - Remove User
  - Change User
  - Browse Unused Ports
  - Browse Dial Ranges
  - Browse Stations
  - Find Unused Extensions
  - Print Button Labels
  - Create New Template
  - Use a template
  - Generate Call-Accounting Data
  - Export Data
  - Import Data
  - Monitor Trunks
  - Find and Replace
- Graphically Enhanced DEFINITY Interface (GEDI), a graphically- enhanced command-line interface. GEDI provides a Windows-style interface to traditional SAT screens, with features such as point-and-click selection and drop-down boxes listing available field values.
- Terminal emulation that provides an interface with the same look and functionality as a traditional SAT.

- Verify/change INTUITY AUDIX administration setup:
  - Net User Password
  - Net User Activate
  - Web Browser – Verify dial plan and extension length
  - Verify node number if networking
- A Windows application that communicates directly with Communication Manager and the INTUITY AUDIX system via a connection through:
  - LAN (TCP/IP) (Technicians connect to the S8100 using a PCMCIA cable to the TN2314)
  - Analog modem
  - Dial in through RMATS port
  - Direct serial connection (RS232 cable, Asynchronous Data Unit [ADU], and so on)

Avaya Site Administration version 1.5 contains additional features:

- Fault and Performance Management Features
  - Trunk Analyzer – Tracks performance and capacity of trunk groups
  - Processor Occupancy and Call Traffic Charting – Tracks processor performance and traffic handling
  - Alarm Monitor – Provides an alerting and reporting mechanism for alarms and errors status
  - Hardware Manager – Allows users to graphically display cabinet information and current alarm status
  - Data Polling Schedule – Lets users easily schedule repeated tasks
  - Generic Device – Supports terminal emulation access to other system types with IP or serial connectivity
  - Communication Manager/PC Time Synchronization – Lets users set up tasks to synchronize their S8100 system clock to the PC's time on a regular basis
  - System Capacity Report – Determines utilization of options and reports them in a consistent manner
  - Manager Audits – Determines if redundant or missing data is administered on a switch
  - Export, Import, and Find and Replace – Export, Import, and Find and Replace functions support INTUITY AUDIX subscribers' data
  - Button Label Printing Enhancements – Lets users print a label from a station template, specify custom button label text, and print bounding boxes with printed labels on plain paper
  - Call Accounting Filtering – Provides advanced filtering capabilities for call-accounting export
  - LDAP Export – Exports to an LDAP directory from supported Communication Manager or INTUITY AUDIX export objects
  - Data Export – Supports more objects than version 1.0, including vector, authorization codes, COR and INTUITY AUDIX subscribers
  - Emulation enhancements – Allows customers to define send break, copy, paste, change text color, and change font

- Enhancements to Reporting – Prints, or exports to a file, a screen capture of any switch command
- Importing Enhancements – Imports from a file into the data import grid
- Port Browser Enhancements – Includes the board's description (such as digital line, 24-port, 2-wire DCP port)

You might encounter either version 1.0 or 1.5 at customer sites. Although customers are responsible for using Avaya Site Administration to add devices, upgrade Avaya Site Administration, and administer the switch, voice technicians and maintenance teams must know how to successfully install and test Avaya Site Administration, which includes:

- Knowledge of Microsoft Windows environment, especially Windows 2000
- How to install the Avaya Site Administration product
- How to test (for example, test a login, access a switch, print a button label, cut through to legacy switch or INTUITY AUDIX)
- How to ensure customer acceptance
- High-level knowledge of contents of available documentation, including on-line documents

In addition, Field Technicians will be responsible for analyzing and correcting problems reported by the customer and must know how to use Avaya Site Administration for problem resolution.

The Avaya Site Administration Help system contains software-embedded documentation to help install and troubleshoot the system, including:

- Avaya Site Administration task-oriented online help
- Avaya Site Administration online help reference
- Installation wizard
- Avaya Site Administration connectivity troubleshooting help topics
- Communication Manager task-based help topics
- Communication Manager reference topics, using the *Administrators Guide for Avaya Communication Manager* (555-233-506)

Interactions with switches and voice-mail systems

Avaya Site Administration is not client-/server-based. It communicates directly with switches and INTUITY AUDIX systems as follows:

- Through a direct hardware connection within an S8100 computer
- Over a LAN
- With a modem or data module

S8100, as shipped, allows installation personnel to connect to switches and voice-mail systems through the direct hardware connection in the S8100 computer. To optimize the efficiency of S8100 and Avaya Site Administration, and because administrators may not want to work directly on the S8100 computer, install Avaya Site Administration software on a separate computer and connect to the switch in any of the other 3 ways listed above.

If installation personnel choose to install Avaya Site Administration on a separate computer, that computer must fulfill the following requirements:

- Windows 95 or 2000 configuration:
  - Processor: 486/Pentium
  - RAM: 16 MB / 32 MB
  - Available Disk Space: 100 MB minimum
  - CD-ROM
  - Printer port: Standard PC printer port or LAN connection
  - Available Serial Ports: 1 free serial port or LAN connection is required for a connection to the switch
  - TCP/IP LAN: Optional, depending on configuration
  - Display: SVGA with minimum screen resolution of 800 × 600

Setting up a voice-mail account is part of the Avaya Site Administration User Administration wizard. For every other INTUITY AUDIX task, administrators must use Avaya Site Administration's terminal emulation feature to open an INTUITY AUDIX terminal emulation window.

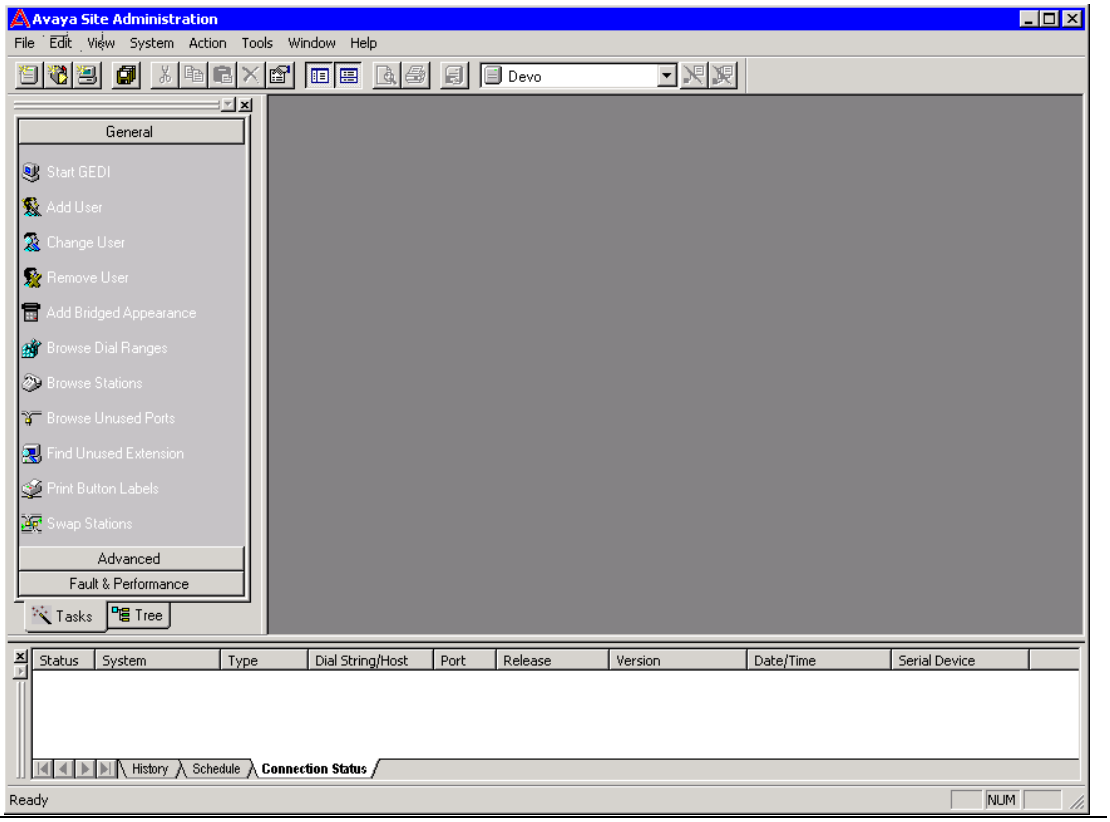
In addition to the switch-administration functions, Avaya Site Administration has its own administration activities. These activities help set up Avaya Site Administration to communicate with switches and INTUITY AUDIXes, organize telecommunications data, and specify that Avaya Site Administration will work. These Avaya Site Administration administration activities include:

- Setting up direct, modem/data module, and LAN connections between Avaya Site Administration and switches or INTUITY AUDIX systems
- Entering Avaya Site Administration-specific data, such as time-out intervals, number of times to retry tasks, and other system options
- Using the history, schedule, and connection viewers to track the status of administration tasks
- Organizing systems and task shortcuts in the browser tree

Components of Avaya Site Administration

Avaya Site Administration provides a central window that allows access to switches and INTUITY AUDIX systems. Figure 49, Avaya Site Administration window with tasks pane and status viewer or history pane, on page 250 shows the main Avaya Site Administration screen.

Figure 49: Avaya Site Administration window with tasks pane and status viewer or history pane



As a default setting, the left pane shows the task wizards that Avaya Site Administration offers for performing frequent tasks. Users can use task wizards to create common tasks and schedule those tasks to run on the system and/or save the tasks to the Avaya Site Administration browser tree. Users can create the following tasks with the task pane:

- Start GEDI – Any administration activity that can be accomplished with the Graphically Enhanced DEFINITY interface (GEDI), including almost all S8100 administration
- User Administration – Add phones, remove phones, and change a phone user's name in S8100 and INTUITY AUDIX
- Find and Replace – Change, find, or remove something across an entire switch
- Import Data – Copy and paste data from a spreadsheet to a grid in Avaya Site Administration
- Export Data – Save switch data to an external file
- Use Template – Add objects, such as a phone, to a switch, using an existing template
- Create New Template – Create a template to use when adding objects to the switch
- Add Bridged Appearance – Create a bridged call appearance on a phone
- Generate Call Accounting – Select call-accounting data and save it as an external file
- Browse Dial Ranges – View the dialing ranges specified by a switch's dial plan
- Find Unused Extension – Search a switch for the next available extension after a specified extension
- Browse Unused Ports – View a list of unused ports on a switch

- Browse Stations – View a selected or complete list of stations on a switch
- Monitor Trunks – Tell Avaya Site Administration to periodically check for out-of-service trunks and notify the user
- Start Emulation – Access a switch or INTUITY AUDIX via terminal emulation
- Add Switch – Set up a connection from Avaya Site Administration to an S8100/G600/CMC1
- Add Voice-Mail System – Set up a connection from Avaya Site Administration to an INTUITY AUDIX system
- Print Button Labels

Clicking the **Tree** tab on the left pane displays the Avaya Site Administration browser tree. This tree is a Windows Explorer-like view of every switch and INTUITY AUDIX system connected to Avaya Site Administration, the tasks a user has created, and the button-label templates. Users can:

- Expand nodes in the tree
- Move items
- Cut, copy, or delete items
- Add or paste items to the tree
- Rename items
- Change an item's properties
- Connect to a switch

How Avaya Site Administration works

In Avaya Site Administration, any switch or INTUITY AUDIX administration activity is called a task. When using Avaya Site Administration to perform a switch or INTUITY AUDIX administration task, enter the task into Avaya Site Administration and then tell Avaya Site Administration when to run the task. For example, to add a phone to the system for a new employee, create a task in Avaya Site Administration that adds the phone (and, optionally, the associated voice-mail account), and then tell Avaya Site Administration to add the new phone immediately or at a later time.

When the task runs, Avaya Site Administration connects to the appropriate switch or INTUITY AUDIX, runs the task, and displays feedback about the task in the schedule tab. Depending on the instructions from the user, Avaya Site Administration will either disconnect from the switch or make the connection idle when it is finished running the task.

Avaya Site Administration help

Avaya Site Administration provides the following information to help administrators:

- Guided tour – The guided tour orients users to the Avaya Site Administration interface, explains what the different areas of the Avaya Site Administration screens are for, and orients users to what Avaya Site Administration is and how to get started. Users can launch the guided tour by choosing Guided Tour from the Help menu.

- Online Help with Demonstrations – The online help system tells how to administer Avaya Site Administration, how to perform basic switch administration and troubleshooting, and how to connect to an INTUITY AUDIX. Many topics include a **Show Me** button. When a user clicks **Show Me**, a short animated demonstration of the task plays. To open the help system, choose **Contents** from the **Help** menu.
- Show Me demonstrations – Users can launch a list of Show Me demonstrations by choosing **Show Me** from the **Help** menu.
- Connection support – Clicking **Help** on a connection error message will launch a series of troubleshooting screens to walk users through solving common connection problems.

Install Avaya Site Administration

If you do not have Avaya Site Administration on your computer, make sure your PC or laptop first meets the minimum requirements described in Table 35, Minimum requirements to run Avaya Site Administration, on page 252:

Table 35: Minimum requirements to run Avaya Site Administration

Operating systems	**Processor/RAM**
MS Windows 2000:	Pentium – 32 MB Pentium – 64 MB
MS Windows XP/ME:	Pentium – 300 MHz, 64 MB Pentium 3 – 600 MHz, 256 MB
Graphics adapter	SVGA with minimum screen resolution of 800 × 600
Diskette drive	3½-in, 1.44-MB floppy disk drive
CD-ROM	CD-ROM drive (required to install Avaya Site Administration from CD)
Available hard disk space	At least 100-MB free hard disk space – This requirement depends on the size and number of configuration data sets.
Printer port	Standard PC or network printer port is required for connecting to a printer to produce station button labels.
Network adapter	Required for network access to the Avaya Media Server, AUDIX, and other network-connected systems.
Free serial ports	One free 9600-bps serial port for connecting to each serial device. We recommend that PCs have at least a 16550A UART (or a 16550A UART simulator, capable of 56-kbps DTE-speed connections – The USB and internal modems should emulate this hardware.) A second serial port is required for a simultaneous serial connection to AUDIX.

You can download Avaya Site Administration to your computer from the Avaya Site Administration software CD. Place the Avaya Site Administration software CD in the CD-ROM drive and follow the installation instructions in the Install Wizard. Use the Online Help for the procedures to establish a switch (media server) record. Use the IP address of the media server and port **5023**.

To start Avaya Site Administration, click **Start** → **Programs** → **Avaya Site Administration**. Avaya Site Administration supports a terminal emulation mode, which is directly equivalent to SAT command interface. Avaya Site Administration also supports a whole range of other features, including the GEDI and Data Import. For more information, see the Online Help, Guided Tour, and Show Me accessed from the Avaya Site Administration Help menu.

Configure Avaya Site Administration

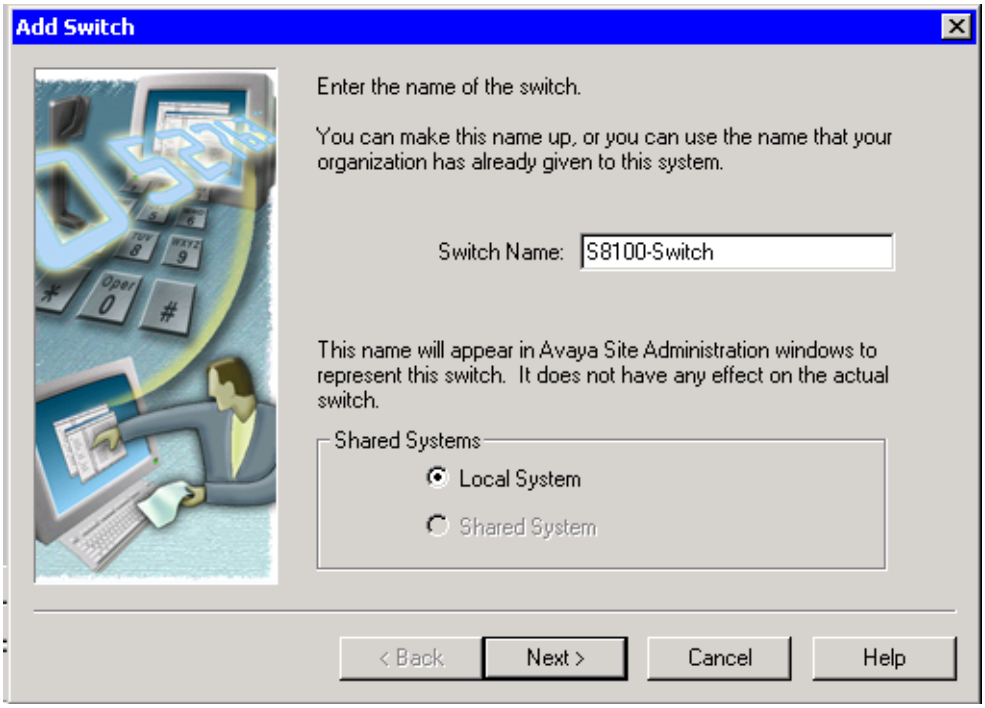
When Avaya Site Administration is initially installed on a client machine, it needs to be configured to communicate with both Communication Manager and the voice-mail applications (INTUITY AUDIX) on the S8100/G600/CMC1 platform.

When it runs initially, after downloading, Avaya Site Administration asks if it should create a new entry for the switch. To create new entries for the switch and voice-mail system, follow these procedures:

- Add an S8100 switch-administration item on page 253
- Add S8100 voice-mail administration item on page 254

Add an S8100 switch-administration item

1 Click **file** → **new** → **Switch**. A screen similar to the following displays:



2 Enter a name in the `Switch Name:` field. As a technician configuring Avaya Site Administration on your laptop, use a generic name, as you will be able to use this connection item for every S8100 machine connected over the PCMCIA physical connection.

3 Click **Next**. The connection type dialog displays.

4 Regardless of the physical connection used (local monitor/keyboard/mouse, PCMCIA, RAS modem or customer LAN) the connection type is always a **Network connection**. Click the **Network connection** radio button.

5 Click **Next**. The Network Connection/IP Address dialog displays.

6 Enter the IP address used to connect to the S8100.

7 Click **Next**. The Network Connection/Port Number dialog displays.

8 Port: For the port number, ALWAYS use port 23.

9 Click **Next**. The Network Connection/Timeout Parameters dialog displays. Leave the default values for the timeout parameters.

10 Click **Next**. The login type dialog displays.

11 Click the "I want to login manually each time" radio button.

12 Click **Next**. The switch summary dialog displays.

13 Check the information, use the Back button to make corrections if necessary, and click the Test button to test the connection.

14 When the connection is successfully tested, click **Next** and then **Finish**.

Add S8100 voice-mail administration item

1 For a new voice-mail administration item, click **File** → **New** → **Voice Mail System**. The Add Voice Mail System screen displays.

2 Enter a name in the **System name** field.

For technicians who are configuring Avaya Site Administration on their laptops, use a generic name, as you will be able to use this connection item for every S8100 machine connected over the PCMCIA physical connection.

3 The remainder of the procedure to add a voice-mail item is the same as adding a switch item – See Add an S8100 switch-administration item on page 253. Enter the connection information for the voice-mail system.

Start a switch-administration session

To launch a GEDI session:

1 Click the tree tab of the Avaya Site Administration window.

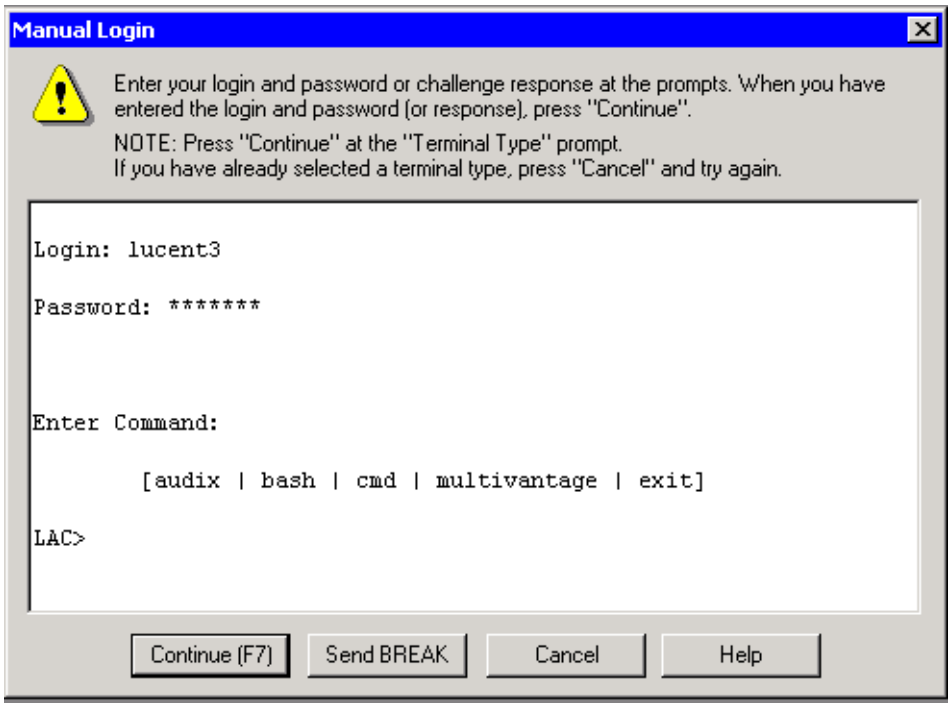
2 Right-click the newly created switch item (S8100 switch in our example).

3 Click **General**.

4 Click **Start GEDI**.

Once the connection has completed, a login screen displays.

5 Enter the login ID and password:



To launch an emulation session:

1 Click the **Tree** tab of the Avaya Site Administration window.

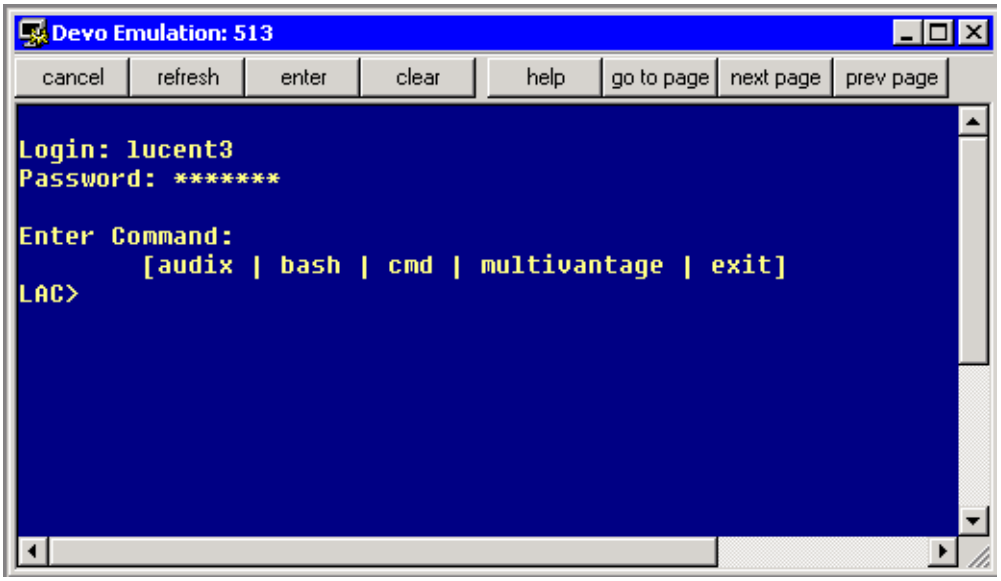
2 Right-click the newly created switch item (S8100 "- Switch").

3 Click **Advanced**.

4 Click either **4410 Emulation** or **513 Emulation**.

Once the connection has completed, a login screen displays.

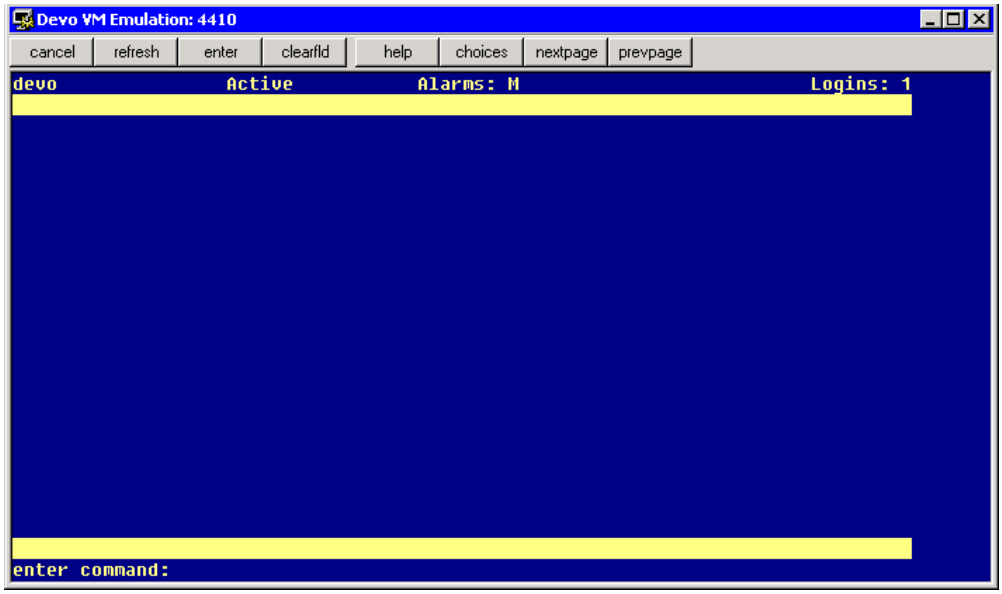
5 Enter the login ID and password:



Start a voice-mail administration session

1. Login to the S8100 system as in the previous procedures – To launch a GEDI session: on page 254 or To launch an emulation session: on page 255.
2. Enter **audix** at the LAC prompt.
3. Enter **4410** as the terminal type.

   A screen similar to the following displays:



8 Message Manager

Avaya Message Manager is a tool for handling multimedia messages with use of a personal computer (PC). Message Manager provides a graphical user interface to access the INTUITY AUDIX messaging system through a local area network (LAN) connection. When connected to a LAN, the INTUITY AUDIX system is referred to as the "INTUITY AUDIX server".

A web-based tool for handling multimedia messages is available as a separate product from Avaya. The product, www.messenger, provides web access to the INTUITY AUDIX messaging system. Contact your Avaya representative for more information.

This chapter provides the high-level steps for downloading the Message Manager software from the S8100 system via the web interface and for installing the Message Manager software on a PC.

For further information about Message Manager features and installation, see *Avaya Message Manager, Release 5.0, Administration*, 555-313-513.

Download Message Manager

The steps required to obtain the Message Manager software from the S8100 system are as follows:

1. On the desktop where Message Manager is to be installed, activate your favorite browser and bring up the home page for the S8100 system.
2. On the S8100 home page, click **User Services**.
3. Use lucent3 for the login ID and password.
4. Click the **Message Manager** link.
5. In the File Download window, click Save to download a self-extracting file to the desktop.
6. In the Save As window, browse to a temporary folder (or click the new folder icon to create a new folder) and click Save. The self-extracting file will be saved in the specified folder.

Install Message Manager

To install Message Manager, first unzip the self-extracting file downloaded in the previous section, then run the setup wizard.

1. Exit every application on the desktop and double-click the self-extracting file downloaded in the previous section, Download Message Manager on page 257.
2. Specify a folder to hold the unzipped files. This can be the same temporary file you are currently in, which holds the self-extracting file. Browse to this folder and click the **Unzip** button.

   The Setup.exe file is extracted, along with some documentation files.
3. Double-click the Setup.exe file. The Avaya Message Manager Installation wizard starts.

4 Follow the prompts to complete the installation:

- In the “Tell Me About” window, click the **Continue** radio button. You can first click the Install Overview or other radio buttons to read about the installation requirements and available documentation, but you will eventually need to click the Continue button to proceed with the installation.
- In the “Install Type” window, click the **Single User Install** radio button.
- In the “Select Destination Directory” window, specify the folder in which to install the software. You can accept the default or browse to (or create) a different folder. For example, *C:\Program Files\Avaya\Message Manager.*
- In the “Backup Replaced Files?” window, click the **Yes** radio button.
- In the “Select Components” window, check **Message Manager** and, optionally, **FAX**.
- If you selected FAX, the enter FAX Information window appears. If you know the Message Server ID and Mailbox Extension, enter them in the space provided. If you don’t know these, you can enter them later.
- Click **Next** in the “Ready to Install” window. The installation will take a few minutes. During the installation, a DOS command window may appear temporarily.
- When the installation finishes, you will be given the option to restart your computer. Click **OK**.

9 Troubleshooting

This chapter provides information about troubleshooting installation problems for S8100. Problem types can:

- Be new and never worked through before
- Occur after installation
- Occur after installation has worked

The following sections apply:

- Install wizard's error messages on page 259
- Platform's troubleshooting commands on page 261
- Modem's configuration and administration on page 262

Install wizard's error messages

Error messages can occur with the S8100 Install wizard. The following table list these error messages and their possible explanations and remedies.

Error message	Possible explanation/remedy
Unable to set the registry default root to HKEY_LOCAL_MACHINE	The registry key HKEY_LOCAL_MACHINE is not accessible from the **install** wizard. Ensure that the registry key is accessible.
S8100 is still running. Shut it down and restart install.	**Install** wizard cannot execute while S8100 applications are running. The command, **shutdown all**, shuts down the applications related to S8100. After this command executes, run the **install** wizard again.
Unable to shut down the CornerStone logger. Manually shut it down and restart the install program.	Execute: **C:\\LucentSoftware\CornerStone\mtce\bin\csShutdownlog.exe**. Execute the command: **C:\\LucentSoftware\CornerStone\bin\cslog_server.exe -UnregServer**. The CornerStone logger should shut down. Run the **install** wizard again.
Unable to register the following files xxxx,yyyy,.....	The **install** program is unable to self-register the files. Register the DLLs manually using the command **regsvr32**.
Unable to reboot workstation now	Install wizard unsuccessfully tried to reboot the workstation. Reboot was attempted because some files were not installed properly (may be in use). Manually push the shut-down switch on the front of the TN2314 and power cycle.

Error message	Possible explanation/remedy
Unable to set xxxx:yyyy from [ffff]	Install wizard could not read the key yyyy from section xxxx in the ini file ffff. Check: • The ini file ffff should be in the same directory as **Setup.exe** (**install** wizard). • The ini file ffff should have read permissions. • The ini file ffff has the section xxxx and a value for the key yyyy.
Unable to determine screen resolution	Escalate.
Screen resolution must be at least 640 × 480.	**Install** wizard requires that the screen resolution be at least 640 × 480.
Unable to determine the operating system	Escalate.
Unable to determine operating system version	Escalate.
Operating system must be Windows 2000 Server.	The underlying OS is not Windows 2000 Server.
Must have administrator privileges to run this program	Installer does not have administrative privileges.
Unable to get free disk space on X drive	Escalate.
Not enough space on X drive for new install. Space required is Y.	Free up space, and ensure that there is at least Y MB space on drive X.
Not enough space on X drive for an upgrade. Space required is Y.	Free up space, and ensure there is at least Y MB space on drive X.
Unable to parse path	Escalate.
Unable to remove last slash from path	Escalate.
Unable to get current path	Escalate.
Unable to create [XXXX]	Escalate.
Unable to create a target directory	Ensure that the path is syntactically correct and you have access rights to the target drive.
Unable to allocate memory required to complete the copy file process	Free memory by terminating as many running applications as possible.
Not enough disk space on target drive to copy the files	Free disk space on target drive.
Unable to open the input file	Ensure that the source file has a valid file name, and that the source file and target directory exist.
Unable to copy the requested file	Escalate.
Target file is read-only	Remove read-only attribute from target file, and try again.

Error message	Possible explanation/remedy
A self-registering file did not register successfully.	Escalate.
Unknown error	Escalate.
Unable to copy file [X]	Escalate.
Unable to get directory name	Escalate.
Unable to parse directory	Escalate.
Unable to create Substring section list	Escalate.
Unable to open file X	Escalate.
Unable to merge [X] into the Registry	Escalate.
Translation ID interval expiration	Login INADS. Reset Translation ID. Save Translation.

The following warnings (insignificant errors) may be generated by the **installconfig wizard**. Attempt to manually resolve these. Note them in the log book and continue. They are:

- Unable to get the INTUITY AUDIX extension length
- Unable to add Avaya Site Administration shortcut to Start Menu
- Unable to reset INTUITY AUDIX extension length to xxxx
- Unable to get file size
- Unable to get the product version from the last install
- Unable to create directory

Platform's troubleshooting commands

For a complete list of commands, see Avaya (Lucent) access controller bash commands on page 329. Detailed strategic analysis of each command is found in *S8100, Maintenance for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways* (555-233-149).

Modem's configuration and administration

The following procedures describe how to check settings and test the external modem:

- Verify INADS modem settings on page 262
- Verify external modem option settings on page 262
- External modem not used on page 263
- Configure the installed modem on page 264
- Test the external modem on page 264

NOTE:
The modem (US Robotics model) is preconfigured to work correctly.

Verify INADS modem settings

No external modem installed

If an external modem is not connected to INADS (no INADS Alarm Origination), proceed as follows:

1. Enter **display system-parameters maintenance**, and press Enter.
2. Verify that the Alarm Origination Activated to OSS Numbers field is set to **n**, and press Enter.
3. Verify that Cleared Alarm Notification and Restart Notification are set to **n**.
4. Test remote access port to **n**.

External modem installed

1. Enter **display system-parameters maintenance**, and press Enter.
2. Verify that the Alarm Origination Activated to OSS Numbers field is set to **y**, and press Enter.
3. Verify that the Cleared Alarm Notification and Restart Notification fields are set to **y**.
4. Test remote access port to **n**.

Verify external modem option settings

1. Connect to the S8100 desktop.
2. Click **Start** → **Settings** → **Control Panel**.
3. Double-click **Phone and Modem Options**.
4. Open the **Modems** tab.

   Verify that the modem's port is attached to COM1.
5. Select the US Robotics 33.6K FAX Ext modem, and click the **Properties** button.

   Verify that the:

   — Speaker's volume is set to mid-range

   — Wait for Dial Tone before Dialing box is checked

6 Click the **Advanced** tab.

7 Click the **Advanced Port Settings** button.

8 Click the **Defaults** button and then the **OK** button.

9 Click the **Change Default Preferences...** button, then click the **Advanced** tab.

10 Verify that the defaults are set:

- **Data bits** is 8
- **Parity** is none
- **Stop bits** is 1
- **Modulation** is Standard

11 Click **OK** three times to save and exit.

External modem not used

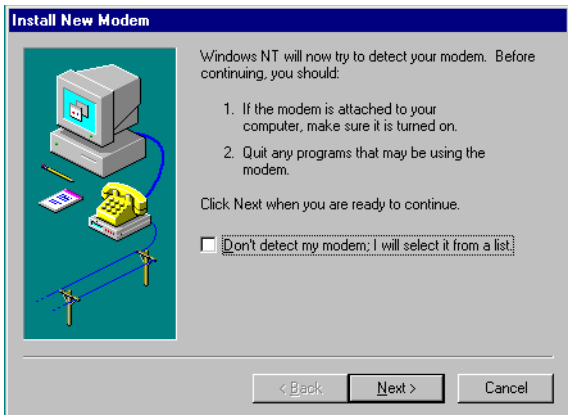
NOTE:
This procedure is necessary if the factory-shipped modem is not used.

1 Connect to the S8100 desktop.

2 Click **Start** → **Settings** → **Control Panel**.

3 Double-click **Phone and Modem Options**.

The **Install New Modem** wizard is displayed:



4 Click **Don't detect my modem. I will select it from a list**.

5 Click **Next**.

6 Click **Add**.

7 Select the manufacturer (3COM Corp) and the model (US Robotics 33.6K FAX Ext).

8 Click **Next**.

9 Select the port the modem is attached to (COM1).

10 Click **Next**.

11 Under "On which ports do you want to install it?, select **Selected ports**.

12 Click **Next**.

The **Modem Setup** screen states that you need to restart the modem before using it.

13 Click **Finish** → **OK**.

Another **Install New Modem** screen states that the modem is set up successfully. The **Modem Properties** screen displays.

Configure the installed modem

1 Right-click **Properties**.

The **Properties** screen displays.

2 Click **OK** to accept speed and speaker volume defaults.

3 Click **Connection** tab.

4 Click **OK** to accept the defaults – for **Data bits** (8), **Parity** (none), **Stop bits** (1), and Call Preference.

5 Click the **Advanced** button.

The **Advanced Connection Settings** screen displays.

6 Click **OK** to accept the defaults.

7 Click **OK** → **Close**.

The **Modem Properties** screen displays.

8 Click **Close**. The following message displays:

```
Dial-up Networking requires configuring because the list of installed
modems has changed. Would you like to do this now?
```

9 Click **Yes**.

10 The **Remote Access Setup** screen confirms that the modem is configured.

Test the external modem

1 At the SAT session, type **change system parameters maintenance**, and click **Enter** or **Submit**.

2 Ensure that the Test Remote Access Port field is set to **y**.

3 Type **test pr-maintenance,** and click **Enter** or **Submit**.

4 Verify that test 230 passes.

For more information see *Administration for Network Connectivity for Avaya Communication Manager* (555-233-504).

10 Security and copy protection

This chapter provides information about software copy protection for an Avaya S8100 Media Server.

Software copy-protection mechanisms

This section provides information about software copy-protection methods for the installation, repair, and upgrade of procedures related to the TSC/COE.

Copying software from one machine to another is more of an issue with S8100's Windows 2000 Server platform running the 3 primary applications (DEFINITY, INTUITY AUDIX, and Avaya Site Administration) than with a proprietary system.

Security measures add a level of impedance (time, money, expertise, etc.) to the process to discourage copying without permission. The possibility exists for someone with physical access to break into a system. There are 2 types of software protection in the S8100 environment: feature and copy protection.

Feature protection

Feature protection has specific feature protection capabilities or capacities within an application. It controls the capabilities provided by the application. As an example, the copy protection for DEFINITY feature translations supports a "customer options" administration form to tailor operation of DEFINITY to a specific customer.

Copy protection

Copy protection prevents software copying. A special mechanism associated with an S8100's license file prevents the software from running on other systems.

A Cable pinouts

This appendix provides the following information for TN760E Tie Trunk and TN464GP T1/E1 option settings, connector and cable diagrams, and pinout charts.

- Set TN760E Tie Trunk's options on page 267
- Set TN464GP T1/E1's options on page 269
- Connector and cable diagrams – pinout charts on page 270

Set TN760E Tie Trunk's options

The TN760E Tie Trunk circuit pack interfaces between 4 tie trunks and the TDM bus. Two tip and ring pairs form a 4-wire analog transmission line. An E & M pair are DC signaling leads used for call setup. The E-lead receives signals from the tie trunk and the M-lead transmits signals to the tie trunk.

To choose the preferred signaling format (Table 36, Signaling formats for TN760E, on page 267 and Table 37, Signaling type summary, on page 267), set the switches on the TN760E and administer the port using Figure 50, TN760D Tie Trunk circuit pack (component side), on page 268 and Table 38, TN760E option-switch settings and administration, on page 268.

Table 36: Signaling formats for TN760E

Mode	Type
E & M	Type I Standard (unprotected)
E & M	Type I Compatible (unprotected)
Protected	Type I Compatible, Type I Standard
Simplex	Type V
E & M	Type V
E & M	Type V Revised

Table 37: Signaling type summary

Signaling type	Transmit (M-lead)		Receive (E-lead)	
	On-hook	Off-hook	On-hook	Off-hook
Type I Standard	ground	battery	open[1]/battery	ground
Type I Compatible	open[1]/battery	ground	ground	open[1]/battery
Type V	open[1]/battery	ground	open	ground
Type V Reversed	ground	open	ground	open

1 An open circuit is preferred instead of battery voltage.

Figure 50: TN760D Tie Trunk circuit pack (component side)

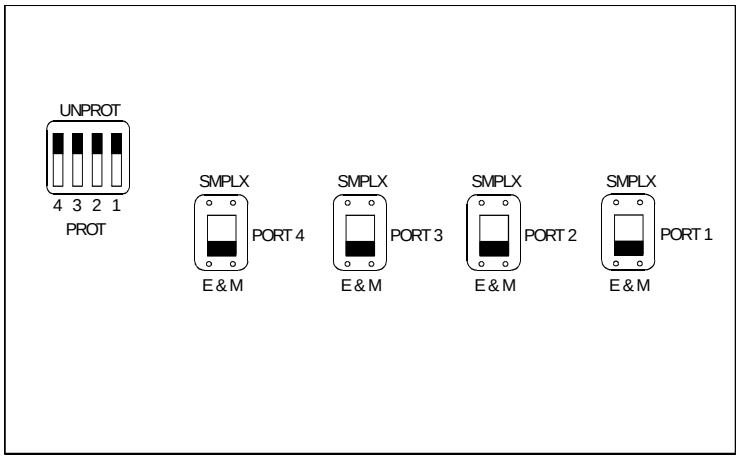


Table 38: TN760E option-switch settings and administration

Installation situation		Preferred signaling format		E&M/SM PLX switch	Prot/Unprot switch	Administered port
Circumstance	**To**	**System**	**Far-end**			
Collocated	Communication Manager	E&M Type 1 Compatible	E&M Type 1 Standard	E&M	Unprotected	Type 1 Compatible
Inter-Building	Communication Manager	Protected Type 1 Compatible	Protected Type 1 Standard Plus Protection Unit	E&M	Protected	Type 1 Compatible
Collocated	Net Integrated	E&M Type 1 Standard	Any PBX	E&M	Unprotected	Type 1

Set TN464GP T1/E1's options

The TN464GP DS1/E1 interface – T1/E1 circuit pack interfaces between a 24- or 32-channel Central Office/ISDN or tie trunk and the TDM bus.

Set the switches on the circuit pack to select bit rate and impedance match. See Table 39, Option-switch settings on TN464GP, on page 269 and Figure 51, Option settings on TN464GP, on page 269. If the top switch setting is set to 32 Channel, set the lower switch setting to either 120 Ohm or 75 Ohm.

Table 39: Option-switch settings on TN464GP

120 Ohms	Twisted pair
75 Ohms	Coaxial requiring 888B adapter
32 Channel	2.048 Mbps
24 Channel	1.544 Mbps

Figure 51: Option settings on TN464GP

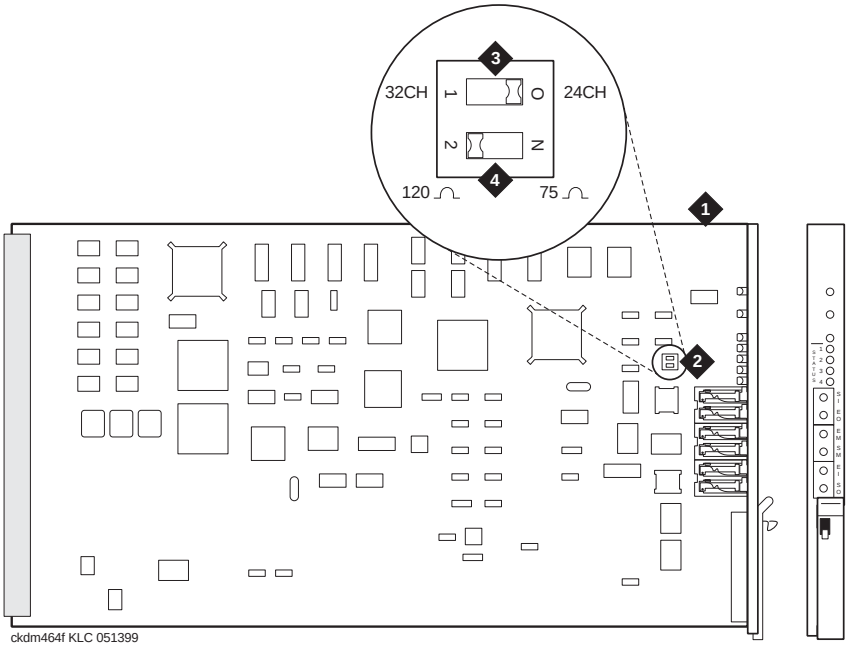


Figure notes

1	TN464GP	**3**	24-/32-channel selector (24CH shown)
2	Option switch	**4**	75-/120-Ohm selector (120 Ohms shown)

Connector and cable diagrams – pinout charts

See Table 40, Lead and color designations, on page 270 for typical lead designations. The circuit packs and auxiliary equipment are classified as shown in the following tables.

Table 40: Lead and color designations ***1 of 2***

Cross-connect pin	Color	Amphenol pin	Backplane pin
1	W-BL	26	102
2	BL-W	01	002
3	W-O	27	103
4	O-W	02	003
5	W-G	28	104
6	G-W	03	004
7	W-BR	29	105
8	BR-W	04	005
9	W-SL	30	106
10	SL-W	05	006
11	R-BL	31	107
12	BL-R	06	007
13	R-O	32	108
14	O-R	07	008
15	R-G	33	109
16	G-R	08	009
17	R-BR	34	110
18	BR-R	09	010
19	R-SL	35	111
20	SL-R	10	011
21	BK-BL	36	112
22	BL-BK	11	012
23	BK-O	37	113
24	O-BK	12	013

1 of 2

Table 40: Lead and color designations ***2 of 2***

Cross-connect pin	Color	Amphenol pin	Backplane pin
25	BK-G	38	302
26	G-BK	13	202
27	BK-BR	39	303
28	BR-BK	14	203
29	BK-SL	40	304
30	SL-BK	15	204
31	Y-BL	41	305
32	BL-Y	16	205
33	Y-O	42	306
34	O-Y	17	206
35	Y-G	43	307
36	G-Y	18	207
37	Y-BR	44	308
38	BR-Y	19	208
39	Y-SL	45	309
40	SL-Y	20	209
41	V-BL	46	310
42	BL-V	21	210
43	V-O	47	311
44	O-V	22	211
45	V-G	48	312
46	G-V	23	212
47	V-BR	49	313
48	BR-V	24	213
49	V-SL	50	300
50	SL-V	25	200

2 of 2

Pinout for Processor's external cable

Table 41: Pinout for Processor's external cable ***1 of 3***

Signal name	Processor (P1) (amphenol connector)	AUX (J1)	Modem (P2)	Mouse	Keyboard	USB	VGA	Ethernet
ACC48A	12	19						
AP1 (alarm in)	2	26						
AP2 (alarm in)	27	27						
EXTALMA	4	48						
EXTALMB	3	23						
XFER48	38	36						
GROUND	25	1						
MOD-CTS	21		5					
MOD-DCD	46		8					
MOD-DSR	8		6					
MOD-DTR	7		20					
MOD-GRD	20		1 & 7					
MOD-RTS	34		4					
MOD-RXD	33		3					
MOD-TXD	45		2					
MOUSE-DAT	18			1				
MOUSE-GRD	31			3				
MOUSE-VCC	6			4				
MOUSE-CLK	5			5				
KYBD-DAT	30				1			
KYBD-GRD	17				3			
KYBD-VCC	16				4			
KYBD-CLK	29				5			
USB-VCC	15					1		
USB-DAT-	40					2		

1 of 3

Table 41: Pinout for Processor's external cable ***2 of 3***

Signal name	Processor (P1) (amphenol connector)	AUX (J1)	Modem (P2)	Mouse	Keyboard	USB	VGA	Ethernet
USB-DAT+	42					3		
GRD	41					4		
VGA-RED	49						1	
VGA-GREEN	47						2	
VGA-BLUE	23							
GRD	10						5	
GRD	48						6	
GRD	46						7	
GRD	24						8	
VGA-PWR	35						9	
GRD	36						10	
VGA-HSYNC	37						13	
VGA-VSYNC	11						14	
ETH-RD+	44							3
ETH-RD-	19							6
ETH-TD+	32							1
ETH-TD-	7							2
RX-	28							
TX+	13							
TX-	14							
RX+	39							
NC	–							
NC	–							
GROUND	50							
NC	–							
–	43							
NC	–							

2 of 3

Table 41: Pinout for Processor's external cable ***3 of 3***

Signal name	Processor (P1) (amphenol connector)	AUX (J1)	Modem (P2)	Mouse	Keyboard	USB	VGA	Ethernet
NC	–							
NC	–							
–	1							

3 of 3

Table 41, Pinout for Processor's external cable, on page 272 shows the pinout for the processor's external cable.

NOTE:
AUX is a 50-pin receptacle, Modem is a 25-pin D-sub plug, Mouse is a 6-pin miniature DIN receptacle, Keyboard is a 6-pin miniature DIN receptacle, USB is a type A receptacle, VGA is a 15-pin D-sub receptacle, and Ethernet is an 8-pin jack.

Table 42: Lead designations for port circuit packs ***1 of 3***

Cross-connect pin	TN742/B TN747B TN753 TN769 TN2147	TN754 TN726	TN760/B TN760C TN760D TN2209	TN762/B	TN763 TN763B TN763C	TN735	TN767B TN464GP TN2207	TN746/B TN2183 TN2215	TN793 TN2793 TN2224/B TN2214
1	T.1		T.1	T.1	T.1	T.1	C_5	T.1	T.1
2	R.1		R.1	R.1	R.1	R.1		R.1	R.1
3		TXT.1	T1.1	TXT.1	SZ.1	BT.1	C_ENAB	T.2	T.2
4		TXR.1	R1.1	TXR.1	SZ1.1	BR.1		R.2	R.2
5		PXT.1	E.1	PXT.1	S.1	LT.1	C_SYNC*	T.3	T.3
6		PXR.1	M.1	PXR.1	S1.1	LR.1		R.3	R.3
7	T.2		T.2	T.2	T.2	T.2	C2D-DATA	T.4	T.4
8	R.2		R.2	R.2	R.2	R.2	RDATA*	R.4	R.4
9		TXT.2	T1.2	TXT.2	SZ.2	BT.2	TDATA*		T.5
10		TXR.2	R1.2	TXR.2	SZ1.2	BR.2	TRSYSNC		R.5
11		PXT.2	E.2	PXT.2	S.2	LT.2	GRD		T.6
12		PXR.2	M.2	PXR.2	S1.2	LR.2	SCLK*		R.6
13	T.3		T.3	T.3	T.3	T.3			T.7
14	R.3		R.3	R.3	R.3	R.3			R.7
15		TXT.3	T1.3	TXT.3	SZ.3	BT.3			T.8

1 of 3

Table 42: Lead designations for port circuit packs ***2 of 3***

Cross-connect pin	TN742/B TN747B TN753 TN769 TN2147	TN754 TN726	TN760/B TN760C TN760D TN2209	TN762/B	TN763 TN763B TN763C	TN735	TN767B TN464GP TN2207	TN746/B TN2183 TN2215	TN793 TN2793 TN2224/B TN2214
16		TXR.3	R1.3	TXR.3	SZ1.3	BR.3	PAHER*		R.8
17		PXT.3	E.3	PXT.3	S.3	LT.3		T.5	T.9
18		PXR.3	M.3	PXR.3	S1.3	LR.3	C_48V	R.5	R.9
19	T.4		T.4	T.4	T.4	T.4		T.6	T.10
20	R.4		R.4	R.4	R.4	R.4		R.6	R.10
21		TXT.4	T1.4	TXT.4	SZ.4	BT.4	C_P2SCLK	T.7	T.11
22		TXR.4	R1.4	TXR.4	SZ1.4	BR.4	LI (RX)	R.7	R.11
23		PXT.4	E.4	PXT.4	S.4	LT.4	LO* (TX)	T.8	T.12
24		PXR.4	M.4	PX4.4	S1.4	LR.4	LBACK1	R.8	R.12
25	T.5		T.5	T.5	T.5	T.5	GND	T.9	T.13
26	R.5		R.5	R.5	R.5	R.5	C_5V	R.9	R.13
27		TXT.5	T1.5	TXT.5	SZ.5	BT.5		T.10	T.14
28		TXR.5	R1.5	TXR.5	SZ1.5	BR.5		R.10	R.14
29		PXT.5	E.5	PXT.5	S.5	LT.5		T.11	T.15
30		PXR.5	M.5	PXR.5	S1.5	LR.5	C_RST	R.11	R.15
31	T.6		T.6	T.6	T.6	T.6		T.12	T.16
32	R.6		R.6	R.6	R.6	R.6		R.12	R.16
33		TXT.6	T1.6	TXT.6	SZ.6	BT.6	RDATA		T.17
34		TXR.6	R1.6	TXR.6	SZ1.6	BR.6	TDATA		R.17
35		PXT.6	E.6	PXT.6	S.6	LT.6	TRSYNC		T.18
36		PXR.6	M.6	PXR.6	S1.6	LR.6	GRD		R.18
37	T.7		T.7	T.7	T.7	T.7	SCLK		T.19
38	R.7		R.7	R.7	R.7	R.7			R.19
39		TXT.7	T1.7	TXT.7	SZ.7	BT.7			T.20
40		TXR.7	R1.7	TXR.7	SZ1.7	BR.7			R.20
41		PXT.7	E.7	PXT.7	S.7	LT.7	GRD	T.13	T.21
42		PXR.7	M.7	PXR.7	S1.7	LR.7		R.13	R.21
43	T.8		T.8	T.8	T.8	T.8	C_PRES*	T.14	T.22
44	R.8		R.8	R.8	R.8	R.8		R.14	R.22
45		TXT.8	T1.8	TXT.8	SZ.8	BT.8		T.15	T.23
46		TXR.8	R1.8	TXR.8	SZ1.8	BR.8	DC2_DATA	R.15	R.23

2 of 3

Table 42: Lead designations for port circuit packs ***3 of 3***

Cross-connect pin	TN742/B TN747B TN753 TN769 TN2147	TN754 TN726	TN760/B TN760C TN760D TN2209	TN762/B	TN763 TN763B TN763C	TN735	TN767B TN464GP TN2207	TN746/B TN2183 TN2215	TN793 TN2793 TN2224/B TN2214
47		PXT.8	E.8	PXT.8	S.8	LT.8	LI* (RX)	T.16	T.24
48		PXR.8	M.8	PXR.8	S1.8	LR.8	LO (TX)	R.16	R.24
49	GRD	GRD	GRD	GRD	GRD	GRD	LBACK2	GRD	GRD
50	GRD	GRD	GRD	GRD	GRD	GRD	GRD	GRD	GRD

3 of 3

* Denotes high side of line.

Table 43: DS1 interface cable H600-307 (or C6C)

50-pin			15-pin		
Pin	**Color**	**Designation**	**Pin**	**Color**	**Designation**
02	W-BL				
03	BL-W				
47	W-G	LI (high)	11	W-G	LI (high)
22	G-W	LI	03	G-W	LI
48	W-BR	LO	09	W-BR	LO
23	BR-W	LO (high)	01	BR-W	LO (high)
49	W-SL	LOOP2	06	W-SL	LOOP2
24	SL-W	LOOP1	05	SL-W	LOOP1

Every other pin is empty.

Table 44, Pinout for TN2185 ISDN-BRI – 4-Wire S interface, on page 277 shows the pinouts for the TN2185 ISDN-BRI 4-wire S interface.

Table 44: Pinout for TN2185 ISDN-BRI – 4-Wire S interface ***1 of 2***

Port	Signal	Cross-connect pin	Color	Amphenol pin	Backplane pin
1	TXT.1	1	W-BL	26	102
	TXR.1	2	BL-W	01	002
	PXT.1	3	W-O	27	103
	PXR.1	4	O-W	02	003
2	TXT.2	5	W-G	28	104
	TXR.2	6	G-W	03	004
	PXT.2	7	W-BR	29	105
	PXR.2	8	BR-W	04	005
3	TXT.3	9	W-SL	30	106
	TXR.3	10	SL-W	05	006
	PXT.3	11	R-BL	31	107
	PXR.3	12	BL-R	06	007
4	TXT.4	13	R-O	32	108
	TXR.4	14	O-R	07	008
	PXT.4	15	R-G	33	109
	PXR.4	16	G-R	08	009
5	TXT.5	17	R-BR	34	110
	TXR.5	18	BR-R	09	010
	PXT.5	19	R-SL	35	111
	PXR.5	20	SL-R	10	011
6	TXT.6	21	BK-BL	36	112
	TXR.6	22	BL-BK	11	012
	PXT.6	23	BK-O	37	113
	PXR.6	24	O-BK	12	013
7	TXT.7	25	BK-G	38	302
	TXR.7	26	G-BK	13	202
	PXT.7	27	BK-BR	39	303
	PXR.7	28	BR-BK	14	203

1 of 2

Table 44: Pinout for TN2185 ISDN-BRI – 4-Wire S interface ***2 of 2***

Port	Signal	Cross-connect pin	Color	Amphenol pin	Backplane pin
8	TXT.8	29	BK-SL	40	304
	TXR.8	30	SL-BK	15	204
	PXT.8	31	Y-BL	41	305
	PXR.8	32	BL-Y	16	205

2 of 2

Table 45, Pinout for TN793 Analog Line circuit pack, on page 278 shows the pinout for the TN793 and TN2793 24-port Analog Line circuit pack.

Table 45: Pinout for TN793 Analog Line circuit pack ***1 of 2***

Port	Signal	Cross-connect pin	Color	Amphenol pin	Backplane pin
1	T.1	1	W-BL	26	102
	R.1	2	BL-W	01	002
2	T.2	3	W-O	27	103
	R.2	4	O-W	02	003
3	T.3	5	W-G	28	104
	R.3	6	G-W	03	004
4	T.4	7	W-BR	29	105
	R.4	8	BR-W	04	005
5	T.5	9	W-SL	30	106
	R.5	10	SL-W	05	006
6	T.6	11	R-BL	31	107
	R.6	12	BL-R	06	007
7	T.7	13	R-O	32	108
	R.7	14	O-R	07	008
8	T.8	15	R-G	33	109
	R.8	16	G-R	08	009
9	T.9	17	R-BR	34	110
	R.9	18	BR-R	09	010
10	T.10	19	R-SL	35	111
	R.10	20	SL-R	10	011
11	T.11	21	BK-BL	36	112
	R.11	22	BL-BK	11	012

1 of 2

Table 45: Pinout for TN793 Analog Line circuit pack ***2 of 2***

Port	Signal	Cross-connect pin	Color	Amphenol pin	Backplane pin
12	T.12	23	BK-O	37	113
	R.12	24	O-BK	12	013
13	T.13	25	BK-G	38	302
	R.13	26	G-BK	13	202
14	T.14	27	BK-BR	39	303
	R.14	28	BR-BK	14	203
15	T.15	29	BK-SL	40	304
	R.15	30	SL-BK	15	204
16	T.16	31	Y-BL	41	305
	R.16	32	BL-Y	16	205
17	T.17	33	Y-O	42	306
	R.17	34	O-Y	17	206
18	T.18	35	Y-G	43	307
	R.18	36	G-Y	18	207
19	T.19	37	Y-BR	44	308
	R.19	38	BR-Y	19	208
20	T.20	39	Y-SL	45	309
	R.20	40	SL-Y	20	209
21	T.21	41	V-BL	46	310
	R.21	42	BL-V	21	210
22	T.22	43	V-O	47	311
	R.22	44	O-V	22	211
23	T.23	45	V-G	48	312
	R.23	46	G-V	23	212
24	T.24	47	V-BR	49	313
	R.24	48	BR-V	24	213
25		49	V/SL	50	314
50		50	SL/V	25	214

2 of 2

Table 46: Classifications of circuit packs and auxiliary equipment

Analog Line (8)	2-Wire Digital & Analog Line (16) and (24)	Data Line & Digital Line 4-wire	Digital Line 2-wire 24-port	Hybrid Line	MET[1] Line	AUX Trunk	Central Office Trunk	Central Office Trunk 3-wire	DID/ DIOD[2] Trunk	Tie Trunk	DS1 Tie Trunk	4-port DIOD[3]
TN467	TN2149	TN726B	TN2224	TN762	TN735	TN417	TN429	TN2199	TN429	TN478	TN483	TN2184
TN432	TN2135	TN754B		TN762B		TN763	TN493		TN2139	TN458	TN722	
TN431	TN468B	TN564B				TN763D	TN422		TN459B	TN449	TN767	
TN411B	TN448	TN413					TN421		TN436B	TN760D	TN722B	
TN742	TN746						TN438B		TN753	TN760C	TN464F	
TN769	TN746B						TN447		TN2146	TN434	TN2207	
	TN2181						TN465C		TN414	TN415	TN2464	
	TN2183						TN747B			TN2209		
	TN793						TN2138					
	TN2793						TN2147C					
	TN2215						TN2148					
	TN791											
	TN2214											

1 MET = Multibutton Electronic Telephone

2 DID/DIOD = Direct Inward Dialing/Direct Inward Outward Dialing

3 DIOD = Direct Inward Outward Dialing

Table 47: Leads for circuit packs and auxiliary equipment (pinout charts) ***1 of 3***

Color	Connector's pin number	8-port Analog Line	16-port, 2-wire Digital or Analog Line	4-wire Data or Digital Line	24-port, 2-wire Digital Line	Hybrid Line	MET Line	AUX Trunk	CO Trunk	3-wire CO Trunk	DID/ DIOD Trunk	Tie Trunk	DS1 Tie Trunk	4-port DIOD Trunk
W-BL	26	T1	T1		T1	V1T1	T1	T1	T1	A1	T1	T1		T1
BL-W	01	R1	R1		R1	V1R1	R1	R1	R1	B1	R1	R1		R1
W-O	27		T2	TXT1	T2	CT1	TXT1	SZ1				T11		
O-W	02		R2	TXR1	R2	CR1	TXR1	SZ11				R11		
W-G	28		T3	PXT1	T3	P-1	PXT1	S1				E1		
G-W	03		R3	PXR1	R3	P+1	PXR1	S11		C1		M1		
W-BR	29	T2	T4		T4	V1T2	T2	T2	T2	A2	T2	T2		T2
BR-W	04	R2	R4		R4	V1R2	R2	R2	R2	B2	R2	R2		R2
W-S	30			TXT2	T5	CT2	TXT2	SZ2				T12		
S-W	05			TXR2	R5	CR2	TXR2	SZ12				R12		
R-BL	31			PXT2	T6	P-2	PXT2	S2				E2		
BL-R	06			PXR2	R6	P+2	PXR2	S12		C2		M2		
R-O	32	T3			T7	V1T3	T3	T3	T3	A3	T3	T3		T3
O-R	07	R3			R7	V1R3	R3	R3	R3	B3	R3	R3		R3
R-G	33			TXT3	T8	CT3	TXT3	SZ3				T13		
G-R	08			TXR3	R8	CR3	TXR3	SZ13				R13		
R-BR	34		T5	PXT3	T9	P-3	PXT3	S3				E3		
BR-R	09		R5	PXR3	R9	P+3	PXR3	S13		C3		M3		
R-S	35	T4	T6		T10	V1T4	T4	T4	T4	A4	T4	T4		T4
S-R	10	R4	R6		R10	V1R4	R4	R4	R4	B4	R4	R4		R4

1 of 3

Table 47: Leads for circuit packs and auxiliary equipment (pinout charts) ***2 of 3***

Color	Connector's pin number	8-port Analog Line	16-port, 2-wire Digital or Analog Line	4-wire Data or Digital Line	24-port, 2-wire Digital Line	Hybrid Line	MET Line	AUX Trunk	CO Trunk	3-wire CO Trunk	DID/ DIOD Trunk	Tie Trunk	DS1 Tie Trunk	4-port DIOD Trunk
BK-BL	36		T7	TXT4	T11	CT4	TXT4	SZ4				T14		
BL-BK	11		R7	TXR4	R11	CR4	TXR4	SZ14				R14		
BK-O	37		T8	PXT4	T12	P-4	PXT4	S4				E4		
O-BK	12		R8	PXR4	R12	P+4	PXR4	S14				M4		
BK-G	38	T5	T9		T13	V1T5			T5		T5			
G-BK	13	R5	R9		R13	V1R5			R5		R5			
BK-BR	39		T10	TXT5	T14	CT4								
BR-BK	14		R10	TXR5	R14	CR4								
BK-S	40		T11	PXT5	T15	P-5								
S-BK	15		R11	PXR5	R15	P+5								
Y-BL	41	T6	T12		T16	V1T6			T6		T6			
BL-Y	16	R6	R12		R16	V1R6			R6		R6			
Y-O	42			TXT6	T17	CT6								
O-Y	17			TXR6	R17	CR6								
Y-G	43			PXT6	T18	P-6								
G-Y	18			PXR6	R18	P+6								
Y-BR	44	T7			T19	V1T7			T7		T7			
BR-Y	19	R7			R19	V1R7			R7		R7			
Y-S	45			TXT7	T20	CT7								
S-Y	20			TXR7	R20	CR7								

Table 47: Leads for circuit packs and auxiliary equipment (pinout charts) ***3 of 3***

Color	Connector's pin number	8-port Analog Line	16-port, 2-wire Digital or Analog Line	4-wire Data or Digital Line	24-port, 2-wire Digital Line	Hybrid Line	MET Line	AUX Trunk	CO Trunk	3-wire CO Trunk	DID/ DIOD Trunk	Tie Trunk	DS1 Tie Trunk	4-port DIOD Trunk
V-BL	46		T13	PXT7	T21	P-7								
BL-V	21		R13	PXR7	R21	P+7								
V-O	47	T8	T14		T22	V1T8			T8		T8		LI*	
O-V	22	R8	R14		R22	V1R8			R8		R8		LI	
V-G	48		T15	TXT8	T23	CT8							LO	
G-V	23		R15	TXR8	R23	CR8							LO*	
V-BR	49		T16	PXT8	T24	P-8							LBACK2	
BR-V	24		R16	PXR8	R24	P+8							LBACK1	
V-S	50													
S-V	25													

3 of 3

The wire colors in this chart apply only to B25A and A25B cables. Colors are not shown for an H600-307 cable.

The following abbreviations apply to every circuit pack, unless otherwise noted:

T,R – PBX transmit voice —— T – Tip (A) Green
T1,R1– PBX receive voice —— R – Ring (B) Red
M – PBX transmit signal —— S – Sleeve
E – PBX receive signal —— PX – PBX transmit
TX – Terminal transmit
LI, LI* – Digital Trunk IN —— LO, LO* – Digital Trunk OUT

The following wire colors apply in the previous chart:

W – White —— S – Slate (Grey)

BL – Blue —— R – Red

O – Orange —— BK – Black

G – Green —— Y – Yellow

BR – Brown —— V – Violet

B Set up customer logins

This chapter provides information about setting up and using customer logins for an S8100 Media Server:

- Customer access on page 285l
- Windows logins for customers on page 286
- Enabling Windows 2000 customer logins on page 290
- Communication Manager logins for customers on page 291

Customer access

The Avaya (Lucent) Access Control (LAC) module allows access to a shell (bash) using any valid Windows 2000 login. This enhancement allows a customer to use a login, such as NTadmin, to access Windows 2000 via a bash shell. This feature is not intended to be used by Avaya Services personnel who continue to use the Lucent Services logins (lucent1, lucent2, lucent3).

Prior to Release 2.0, the LAC module listened only on TCP port 23. A connection to this port produced different results depending on the login used. For example, a services login (lucent1, lucent2, lucent3) resulted in the **LAC** prompt to select Communication Manager, INTUITY AUDIX, or a bash shell. An alias login, such as donut, resulted in a SAT screen without a LAC prompt. This continues to be supported in the May 2003 release, but is being deprecated in favor of the use of separate telnet ports for direct access to embedded AUDIX and INTUITY AUDIX.

If the Telnet session is established to TCP port 22, and the login has privileges to access Communication Manager, a connection is made directly to SAT without a LAC prompt. If the caller logs off, the Telnet session is terminated.

If the Telnet session is established to TCP port 24, and the login has privileges to access INTUITY AUDIX, a connection is made directly to an INTUITY AUDIX Forms Controller administration screen without a LAC prompt. If the caller logs off, the Telnet session is terminated.

The same logins are used with ports 22, and 24, as well as 23. The difference is that a direct connection is made to the appropriate application without a LAC prompt or having to use an alias login.

See Access methods on page 151.

Windows logins for customers

Several Windows login groups and associated logins are preinstalled for customer use from the factory. See Table 48, Windows 2000 logins, on page 286.

The login IDs in the last 2 columns of Table 48, Windows 2000 logins, on page 286 are for customer use. The following describes use and administration of these logins.

Table 48: Windows 2000 logins

Windows login group	Logins for customer use	
	User name	Default password
Administrators	NTadmin	NTadmin1
Guest – disabled	–	–
lucent	–	–
officeadmin	[1]	
officeuser	[2]	
Power Users	–	–
Users	browse vm sa	

1 To be administered

2 To be administered

WARNING:

The logins in the Lucent group of Table 48, Windows 2000 logins, on page 286 are for the exclusive use of Avaya Services personnel. These logins are established and updated automatically by Lucent software. DO NOT ALTER THESE LOGINS IN ANY MANNER. To do so may render the system unserviceable and may require a partial or complete reinstallation of the software by Avaya personnel.

Windows login types for customers

Administrator login

- NTadmin

  This is a standard Windows administrator account used to administer network parameters and similar functions.

INTUITY AUDIX logins

- browse

  This login is used in the Voice Messaging application. See the INTUITY AUDIX documentation or Table 49, INTUITY AUDIX commands versus logins for sa, vm, and browse, on page 287 for a list of commands accessible to the browse login. This login is disabled from the factory. It must be enabled and a password chosen before it can be used. See Set up login accounts on page 290.

- vm

  This login is used in the Voice Messaging application. See the INTUITY AUDIX documentation or Table 49, INTUITY AUDIX commands versus logins for sa, vm, and browse, on page 287 for a list of commands accessible to the vm login. This login is disabled from the factory. It must be enabled and a password chosen before it can be used. See Set up login accounts on page 290.

- sa

  This login is used in the Voice Messaging application. It has full customer administration privileges. See the INTUITY AUDIX documentation or Table 49, INTUITY AUDIX commands versus logins for sa, vm, and browse, on page 287 for a list of commands accessible to this login. This login is disabled from the factory. It must be enabled and a password chosen before it can be used. See Set up login accounts on page 290.

NOTE:
The stand-alone INTUITY AUDIX system login **sa** normally produces a menu. This feature is not supported on S8100. Every login results in a Forms Screen interface.

Table 49: INTUITY AUDIX commands versus logins for sa, vm, and browse ***1 of 2***

Command	Login		
	sa	**vm**	**browse**
add	×	×	
audit	×	×	
change	×	×	
copy	×		
display	×	×	×
exit	×	×	×
get	×	×	
help	×	×	×
list	×	×	×
logoff	×	×	×
print	×	×	×
remove	×	×	
reset	×		

1 of 2

Table 49: INTUITY AUDIX commands versus logins for sa, vm, and browse *2 of 2*

Command	Login		
	sa	vm	browse
test	×	×	×
toggle	×	×	×
trace	×	×	×

2 of 2

Customer's web-access logins

The following login groups are used for web access:

- Officeadmin

  Login IDs in this group are installed from the factory.This login group facilitates access via the S8100 web interface. Group members select administrative privileges via the web interface. The Windows admin account is used to establish an account in this group. Generally, an account in the Offieceadmin group is used to download Avaya Site Administration from the S8100 web page. See Table 50, Web access rights/officeadmin and officeuser access, on page 288.

- Officeuser

  Login IDs in this group are installed from the factory. This login facilitates download of client software, such as Message Manager. Group members have access for client download only. The NTadmin login is used to establish an account in this group. An Officeuser group account is generally used to download Message Manager from the S8100 web page. See Table 50, Web access rights/officeadmin and officeuser access, on page 288.

- anonymous

  The anonymous login is for very limited access via the web interface to load a software patch. See Table 49, INTUITY AUDIX commands versus logins for sa, vm, and browse, on page 287 "INTUITY AUDIX commands versus logins".

Table 50: Web access rights/officeadmin and officeuser access *1 of 3*

Directory	Use	Login group	Permissions
c:\LucentWeb\Public	S8100 Home Page	anonymous	read
		officeuser	read
		officeadmin	read
		administrators	full control
		lucent	full control

1 of 3

Table 50: Web access rights/officeadmin and officeuser access ***2 of 3***

Directory	Use	Login group	Permissions
c:\LucentWeb\admin\audix\html	INTUITY AUDIX networking HTML pages	anonymous	none
		officeuser	none
		officeadmin	read
		administrators	full control
		lucent	full control
c:\LucentWeb\admin\audix\cgi	INTUITY AUDIX networking cgi scripts	anonymous	none
		officeuser	none
		officeadmin	execute
		administrators	full control
		lucent	full control
c:\LucentWeb\admin\user\html	Pages for non administrator users e.g. download	anonymous	none
		officeuser	read
		officeadmin	full control
		administrators	read
		lucent	full control
c:\LucentWeb\admin\user\cgi	cgi scripts for non administrator users. e.g. download	anonymous	none
		officeuser	execute
		officeadmin	execute
		administrators	full control
		lucent	full control
c:\LucentWeb\admin\html	Platform HTML pages	anonymous	none
		officeuser	none
		officeadmin	read
		administrators	read
		lucent	full control

2 of 3

Table 50: Web access rights/officeadmin and officeuser access ***3 of 3***

Directory	Use	Login group	Permissions
c:\LucentWeb\admin\cgi	platform cgi scripts	anonymous	none
		officeuser	none
		officeadmin	execute
		administrators	execute
		lucent	full control
c:\LucentWeb\AdminAll\html	Restricted html pages. e.g. activate Terminal Server	anonymous	none
		officeuser	none
		officeadmin	none
		administrators	full control
		lucent	full control
c:\LucentWeb\AdminAll\cgi	Restricted html pages. e.g. activate Terminal Server	anonymous	none
		officeuser	none
		officeadmin	none
		administrators	full control
		lucent	full control

3 of 3

Enabling Windows 2000 customer logins

Only the Administrator can enable customer logins.

Set up login accounts

1. Start the Windows 2000 user manager on the S8100 desktop. Click **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **Local Users & Groups**.
2. Change the password for the NTadmin account.
3. Activate and set passwords for the browse, vm, and sa accounts. This also can be done via the command line tool **net user**. See Avaya (Lucent) access controller bash commands on page 329.
4. Create 3 Windows accounts in the Officeadmin group for 3 application administrators. These accounts are used to download Avaya Site Administration software. The account names can be chosen as desired. For this example they are called D1user1, D1user2, and D1user3.

5 Create 1 Windows account in the Officeuser group for download of the INTUITY Message Manager Software.The Windows admin account should be used for Windows administration only. The account name can be chosen as desired. For this example it is called D1WEB.

6 Disconnect from Terminal Server.

NOTE:
The Windows admin account can be used for download, but should be used for Windows administration only.

Communication Manager logins for customers

In addition to the logins maintained in the Windows operating system, there are customer level logins within Communication Manager that do NOT appear as Windows logins. The default password should be changed by the customer during installation.

Table 51: Communication Manager customer logins

Communication Manager customer logins	Comments	Default password
defty1	This is the customer level “super user” login within Communication Manager. Its use should be restricted to the system administrator. This login can be used to create additional Communication Manager logins. See the SAT command **add login**.	

The May 2003 release of S8100 provides enhanced login/password security by adding a security feature that allows users to define their own Communication Manager logins/passwords and to specify a set of commands for each login.

- The system allows up to 14 simultaneous connections (logins) to S8100. (S8100 can have 5 connections, INTUITY AUDIX can have 4 connections, and the rest of the connections are reserved for shell commands.)
- Each S8100 login name can be customized
  - — Logins must be 3 to 6 alphabetic/numeric characters, or a combination of both.
  - — A password must be from 4 to 11 characters in length and contain at least 1 alphabetic and 1 numeric symbol.

Password aging is an optional feature that the super-user administering the logins can activate (see the following).

NOTE:
If several users are logging in and out at the same time, a user may see the message: **Transient command conflict detected; please try later.** After the users have completed logging in or out, the terminal is available for use.

Forced password aging

Forced password aging operates as follows:

- The password for each login can be aged starting with the date the password was created, or changed, and continuing for a specified number of days (1 to 99).
- 7 days before the password expiration date, the user is notified that the password is about to expire at the login prompt.
- When the password expires the user is required to enter a new password into the system before logging in.
- If a login is added or removed, the Security Measurement reports are not updated until the next hourly poll, or when a **clear measurements security-violations** command is entered.
- Once a non-super-user has changed the password, the user must wait 24 hours to change the password again.

Logoff notification

Security is enhanced by providing a logoff notification screen to a system administrator at log off while either the facility test call or remote access features are still administered. The administrator can be required to acknowledge the notification before completing the logoff process. Logoff notification is administered on the Login Administration screen.

Super user

Avaya delivers the S8100/G600/CMC1 solution to the customer with 1 customer “super-user” login/password defined. The customer administers additional login/passwords as needed. The super-user login has full customer permissions and can customize any login created.

Login permissions for a specified login can be set by the super user to block any object that may compromise switch security. Up to 40 administration or maintenance objects commands can be blocked for a specified login ID.

Administer login command permissions

Users with super-user permissions can set the permissions of logins they create by performing a **change permissions <login-name>** command. This causes the Login Permissions form to display. The Login Permissions form allows the user to control access to various categories of commands for a given login. It also permits restricting access to objects (forms) on an individual basis for up to 40 objects. Restricting an object means that no commands may be performed on that object by that login (add, change, remove, etc.) The three main categories of commands are:

- Common commands
- Administration commands
- Optional maintenance commands

Each category of commands has sub-categories that, when set to **y,** allow access to objects associated with that sub-category. If the category is set to **n**, the user is not be able to add, remove, or change commands on objects under that sub-category. If the display category is **y**, the login will list or display the object in most cases. If the super-user wants to restrict access to every command associated with an individual object in a subcategory, the Additional Restrictions field is set to **y**. This causes 2 additional pages to be added to the permissions form. Scroll these pages and press **Help**. Individual objects will be displayed in alphabetical order. Enter the object that you want to restrict access to into the fields and submit the form. Up to 40 objects may be restricted. A restricted login cannot access any of the commands associated with that login. Note that permissions cannot be changed for the login and you cannot create Additional Restrictions without full super-user permissions.

Communication Manager commands for user login

Communication Manager commands refer to the set of commands that execute under Communication Manager running on the S8100 Media Server and which can be accessed through a SAT session or the Avaya Site Administration application.

These commands are grouped into three command categories. Each of the three command categories has a group of command subcategories listed under them, and each command subcategory has a list of command objects that the commands acts on. A super-user can set a user's permissions to restrict or block access to any command in these categories. These categories are displayed on the Command Permissions Categories form. The three main categories are:

- Common commands
  - Display administrative and maintenance data
  - System measurements
- Administration commands
  - Administer stations
  - Administer trunks
  - Additional restrictions
  - Administer features
  - Administer permissions
- Maintenance commands
  - Maintain stations
  - Maintain trunks
  - Maintain systems
  - Maintain switch circuit packs
  - Maintain process circuit packs

Password expiration

If your password has expired, the following message displays:

```
          Login: telmgr

       Password:
       Your Password has expired, enter a new one.

    Reenter Current Password:

                New Password:

       Reenter New Password:
```

If your password is within 7 days of the expiration date, the following message displays:

```
WARNING: Your password will expire in x days.
```

C Miscellaneous procedures

The following sections provide miscellaneous procedures used in the S8100 installation process.

- Setting the name of the switch on page 295
- Connect to SAT session via Telnet on page 296
- Installing INTUITY languages other than English on page 299
- Backup and Restore
  - Perform backup on page 302
  - Backup via the web interface on page 305
  - From the backup and restore main menu, you can: on page 307
  - Perform immediate backup on page 308
  - View backup progress on page 309
  - Back up to a LAN address on page 309
  - View scheduled backups on page 311
  - Access backup information on page 311
  - Perform restore on page 313
- Enable/disable embedded messaging on page 314
- Access Diskeeper software to defragment the disk on page 315

Setting the name of the switch

Setting the Windows name

To set the machine name, in a bash shell, type **setip name=machineName**. Limit the machine name to 10 characters. Setip will allow you to enter more characters, however INTUITY AUDIX only displays the first 10 characters of the machine name in its administration window.

Ex: setip name=mysite

After setting the machine name, the **setip** command displays both the old and new settings.

Reboot the S8100. Enter **reboot nice** from a console bash shell.

Updating INTUITY AUDIX machine name

1. Once Windows reboots, Update INTUITY AUDIX. Enable the S8100 web page using a browser. Click the **Administer System** link. The web page prompts for login and password. Use the **lucent3** login with the new password supplied by INADS.
2. Click the INTUITY AUDIX Networking link. Click the Administrative Menu link after the page loads. Click the Local Machine Administration link to load the Local Machine Administration web page. Click the change button in the middle of the page for INTUITY AUDIX to re-populate its databases with the current settings.
3. Exit the web pages and restart INTUITY AUDIX.

Restarting INTUITY AUDIX

Enable a Telnet session to the S8100's LAC bash shell. Execute the **shutdown Audix** command at the shell prompt. Select **start Audix** when the shutdown finishes. When INTUITY AUDIX restarts, it recognizes the new machine.

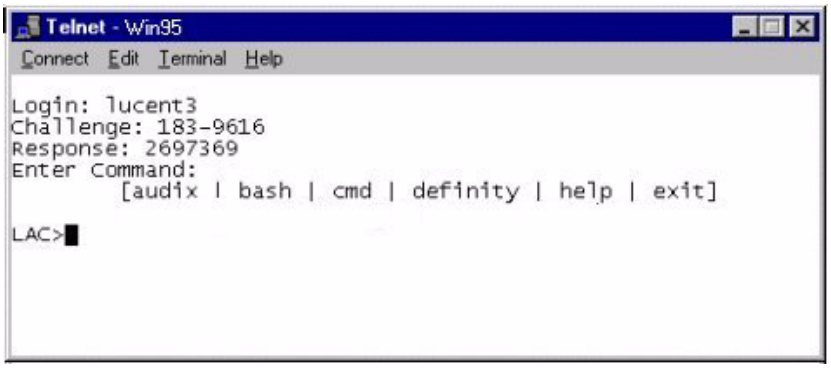
Changing system name

1. When the system is up, enable a SAT session, using either telnet or Avaya Site Administration. Login as **dinit** (lucent1 will grant the same permissions) with the appropriate password.
2. Enter change system-parameters features. On page 4, change the switch name to match the Windows 2000 and INTUITY AUDIX switch names.

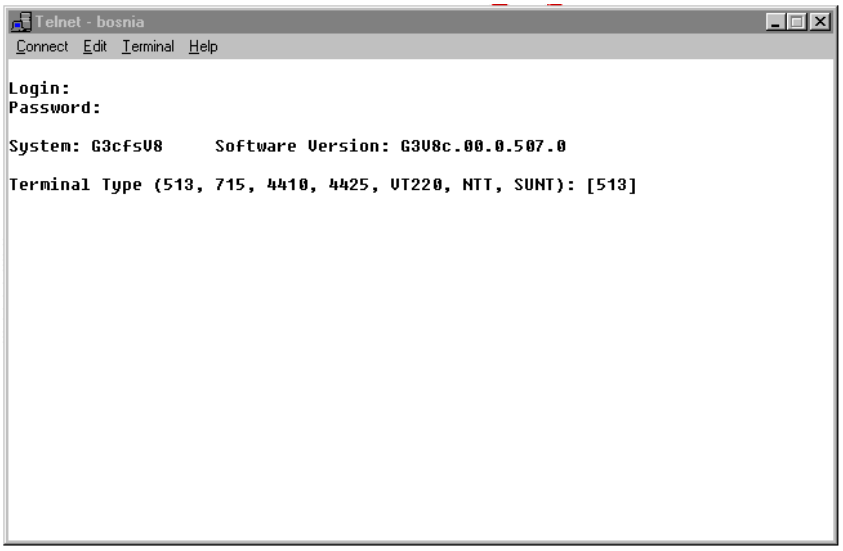
Connect to SAT session via Telnet

This method of access is used primarily by technicians who use one of the services logins. This connection type will access a SAT emulator to administer and maintain the S8100.

1. Enter a command after logging in to the S8100 system. See Via a Telnet session on page 152. In this example, the command entered was **multivantage**. The next screen shows the initial SAT screen.



2 Enter the terminal type.

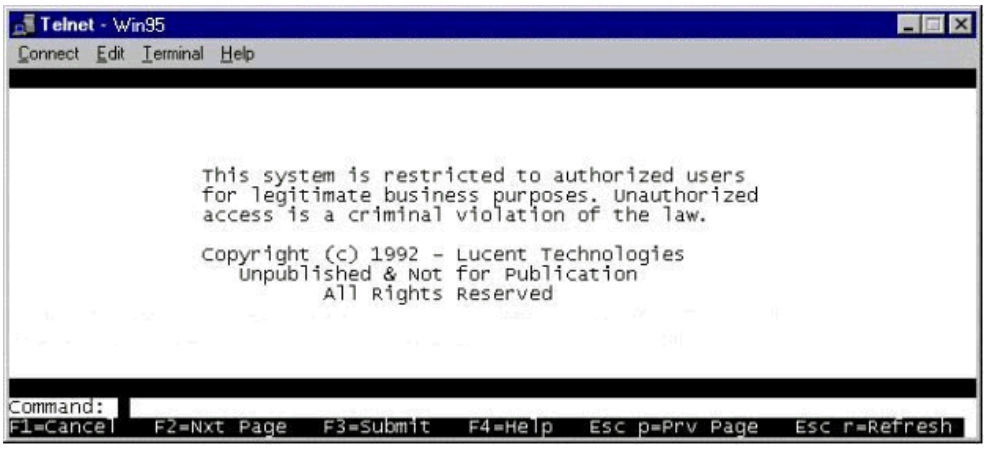


The screen shows login and password fields. You are automatically logged in to the SAT session by the LAC.

NOTE:
Three new terminal types have been added: NTT, W2KTT, and SUNT. W2KTT uses different function-key sequences, see Function-key sequences for W2KTT terminal type on page 298.

- Use NTT from a Windows 95, 98, or NT platform.
- Use W2KTT from a Windows 2000 platform.
- Use SUNT from a Sun Microsystems platform.

The following screen displays when the terminal type is entered:



Once you are logged in as user **lucent1**, **lucent2**, or **lucent3**, you can exit the SAT session and start an INTUITY AUDIX session without having to re-authenticate.

Function-key sequences for W2KTT terminal type

You cannot use the same function-key sequences for SAT on a Windows 2000 platform. However, the 4 arrow keys do work as expected.

NOTE:
Function keys are case-sensitive. For example, **Esc p** and **Esc P** produce two different results.

Use the following Escape-key sequences when using the W2KTT terminal type:

Action	Key sequence
Refresh	Esc r
Cancel	Esc x
Submit	Esc e
Logout	Esc l (lower case L)
Clear field	Esc c
Help	Esc h
Next form	Esc f n
Next page	Esc n
Prev page	Esc p
Edit vec	Esc f 6
Dir page	Esc d p
Update form	Esc u f
Next field	Esc N
Prev Field	Esc f p

Installing INTUITY languages other than English

To access the S8100, the technician needs a laptop, a PCMCIA card for the laptop, a 451A adapter, a D8W cord, a cross-over cord, and the CD with the Merrill-Lynch INTUITY AUDIX™ R5.0 Announcement set.

A cord, comcode 846943306, can be used. If this cord is unavailable, a 104 block can be used with 2 D8W cords. Wire the 104 block with the white, orange pair transposed with white, green pair between the jacks. The 3Com™ 3CXFE575BT NIC needed to access the TN2314 is always to be left on site in the correct slot. If everything is connected properly and the laptop is up and running, there will be a green LED lit on the NIC plugged into the TN2314. If there is no LED, recheck the connections.

Verify the CD can be read by the laptop's CD-ROM.

Laptop configuration for Windows 95/98/NT

1. Right click Network Neighborhood, and select **Properties**.
2. Under the ***Configuration*** tab, click **TCP/IP Ethernet NIC**.

   NOTE:
   The services laptop uses a Zircom card.

3. Click **Properties**.
4. Select the ***IP Address*** tab.
5. Record the *IP Address* and *Subnet Mask*, if any. These will be needed later.
6. Change the *IP Address* to 192.11.13.5 and the *Subnet Mask* to 255.255.255.252; then click **OK**.
7. Click **OK** in the Network window.
8. When the system says to click **OK** for the settings to take effect, do so.
9. Click Start, Settings, and select **Control Panel**.
10. Double-click **Display**.
11. Select the **Screen Saver** tab, and set the screen saver to **None** until the upgrade finishes.

CAUTION:
If the laptop's screen saver is not disabled and times out during the upgrade, the Terminal Server™session will drop. The technician will have to wait approximately 5 minutes to re-establish the connection. The upgrade will continue without any ill effects, even though the session has dropped.

NOTE:
For Windows NT™and Windows 2000™, be sure that NETBUI is installed on the Protocols tab under Properties. Otherwise the computer will not be recognized by the system. This will affect mapping a drive for doing upgrades. If you connect to the AVAYA network, you may have to disable NETBUI after you are finished working on the system.

NOTE:
For Windows™ NT and Windows 2000™, follow the above procedure; however, the laptop my not ask to be rebooted for settings to take effect (as in step 8, above). This should be done, in any case.

For Windows™2000, there have been some changes:

1. Right click My Network Places, and select **Properties**.

   This opens the ***Network and Dial-up Connection*** window.
2. Right click the Local Area Connection, and select **Properties**.
3. In the ***Connect Using*** window, select the **General** tab.
4. Click Internet Protocol (TCP/IP) in the lower portion of the window.
5. Click Properties, which is now selectable.
6. If there is an IP address in the next window, write it and any other information down. These will be needed later.

   NOTE:
   If the following IP address does not have a dot in it, click it.
7. Change the *IP Address* to 192.11.13.5 and the *Subnet Mask* to 255.255.255.252.

   NOTE:
   If there is anything in the DNS, the system needs to be rebooted for the changes to take effect.
8. Click **OK**.
9. Close the windows and reboot the system, if necessary.
10. Connect the cross-over cable between the laptop and the TN2314 Service Access port (RJ-45 jack).

CAUTION:
When using Terminal Server™, because of the size of the laptop display, use the scroll bar on the right side of the display to go to the bottom of the desktop screen. That is where the Start button for the desktop is found. Otherwise, the Start button on the Taskbar may be that of the laptop. The technician can also right click the laptop Taskbar, select Properties, and check the Auto Hide box. This will cause the Taskbar to be hidden until the cursor is moved to the very bottom of the display.

Installing INTUITY languages

Perform the following procedures:

1. Insert the CD into the laptop; then open ***My Computer*** on the laptop.
2. Click CD-ROM.
3. Right click CD-ROM, and select **Sharing**.
4. Under ***Sharing***, click **Share As** and give the drive a name, like *Upgrade*.

   NOTE:
   After the upgrade finishes, you can discontinue sharing the CD-ROM.

5. Click **OK**, and close ***My Computer*** to return to the desktop.
6. For Windows™95/98, right click Network Neighborhood, and select **Properties**.
7. Select **File and Print Sharing**.
8. Check *I want to be able to give others access to my files.*
9. Click **OK** in both windows to exit.
10. Connect the laptop to the RJ-45 Access Service port.
11. Start the laptop internet browser.
12. On your browser, turn off proxies. Write down the settings for restoration later.
    - **Internet Explorer™ 4.x** – go to View, Internet Options, Connections; check *Connect to Internet using LAN*; uncheck *Use proxy server.*
    - **Internet Explorer™ 5.x** – go to Tools, Internet Options, Connections. At the bottom of the window, click **LAN Settings**. Uncheck *Use a proxy server* box and *Automatically detect settings*. Click **OK** until back at web page.
13. Execute an http://192.11.13.6
14. Login
15. Click **Administer System**, and Login.
16. Start Terminal Server™on the system by clicking on **Login to S8100** under Remote Control – Terminal Services (“S8100” may have been changed to a different server name).
17. Answer yes to the questions asked on the agreement screens, if they appear.
18. Login
19. Right click My Network Places, and select **Map Network Drive**.
20. The screen appears with a default drive letter. Change this to another letter, like G.
21. Uncheck *Reconnect at Logon*, and click **Finish**.
22. Wait while the system locates the laptop.
23. When the laptop appears, double-click it to display shared drives.
24. Double-click the CD-ROM.

    The path box at the top of the window becomes populated.
25. If a window with the CD-ROM contents does not open, right click the S8100 icon (this looks like the My Computer icon). If the contents appear, go to step number 31.
26. Click **Explore**.

27 Expand the CD-ROM drive by clicking on the + in front of it.

28 Click down using the + on the following folder icons:

- Us-eng
- Cas-span
- French-c
- German
- Lat-span
- setup.exe

29 Click the **setup.exe** icon.

30 In the ***Language Installation*** screen, select the CD-ROM drive as the *Source*, and the D drive as the *Destination*.

31 Click the language to be added.

> **NOTE:**
> The system already has Us-eng, and can have up to three languages installed.

32 Click **Add**.

33 Click **Install**.

34 On the screen that says the installation was successful, click **OK**.

The languages are now installed and can be used.

Perform backup

Backup procedures prevent loss of data due to system errors. Backups can be either immediate or scheduled. You can backup data to either the LAN or the PCMCIA flash card from the command line and web browser.

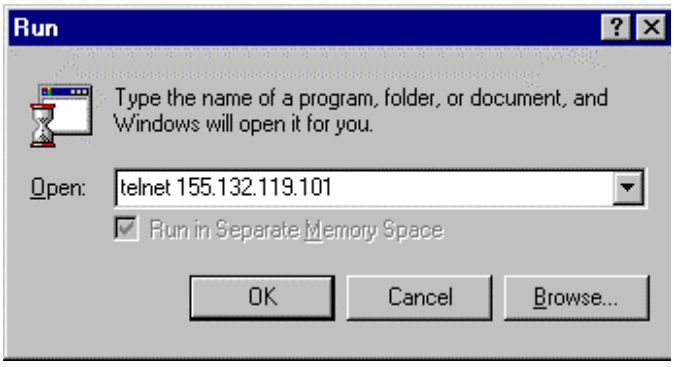
> **NOTE:**
> Avaya strongly recommends that you schedule backups to more than one destination. For example, create one schedule to backup translations to a PCMCIA flash card and another schedule to backup to a different location for each day of the week on a remote hard disk drive on the LAN.

To backup to a flash card, first insert a PCMCIA card into the free slot on the TN2314 circuit pack. For alternative backup, obtain a network location from the customer.

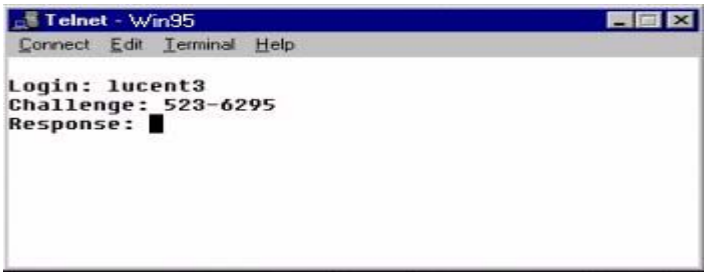
Backup using a LAN-resident PC

This is the bash shell procedure when using a LAN-resident PC that is not S8100 but is connected to the same LAN as S8100.

1. Click **Start** → **Run** from the Windows task bar. The **Run** dialog displays:



2. Enter **telnet {S8100 Name or IP Address}**. Click **OK**.
3. A Telnet session opens on the desktop. Enter the login and response at the prompts.



Once the AVAYA Access Control process accepts your inputs, it grants admittance to the S8100 system.

4. At the LAC prompt, type **bash** and press Enter.

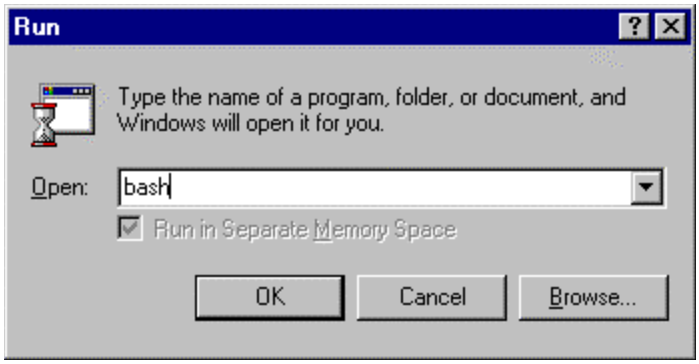
   The machine name and login ID displays as your prompt.

5. Skip to Enter backup commands on page 304.

Backup using an S8100 desktop

This is the bash shell procedure when using an S8100 desktop.

1. At an S8100 desktop, log into Windows.
2. Click **Start** → **Run** from the Windows task bar. The **Run** dialog displays:



3. Enter **bash**, and click **OK**.
4. A Telnet session opens on the desktop. Enter User Name and Password.

   The S8100 system grants admittance once inputs are accepted.
5. Continue with Enter backup commands on page 304.

Enter backup commands

1. Type **d1backup** <**data-set**> <**destination**> and press Enter.
2. Enter one or more of the following data-set parameters (separate multiple choices with a space) for backup:

Parameter	Meaning
deftran	Communication Manager Translations
vmnamtran	Voice Names and Translations
vmmsgtran	Message Bodies and Translations
vmannounce	Announcement Sets
vmnammsgtran	Voice Names, Messages, and Translations
registry	NT registry
sam	NT Passwords Login and Policy
defann	Communication Manager Announcements
lac	Password and License Server File

The destination is **pcmcia** to backup to a flash card, or a directory name to backup to a remote hard disk on the LAN.

If a directory name is entered, a network drive must be mapped as the F: drive. Use the web interface to map a network drive.

The following is an example of how to enter information for backup procedures:

LAC:> **d1backup deftran vmnamtran pcmcia**

NOTE:
When executing this command, there may be a delay of 1 to 2 minutes because INTUITY AUDIX Networking is shutting down and auditing the INTUITY AUDIX databases. INTUITY AUDIX restarts when the backup completes.

Backup via the web interface

The following are web-interface procedures:

1. Open Internet Explorer.
2. Enter **http://<IP address>** in the address area of the web browser.

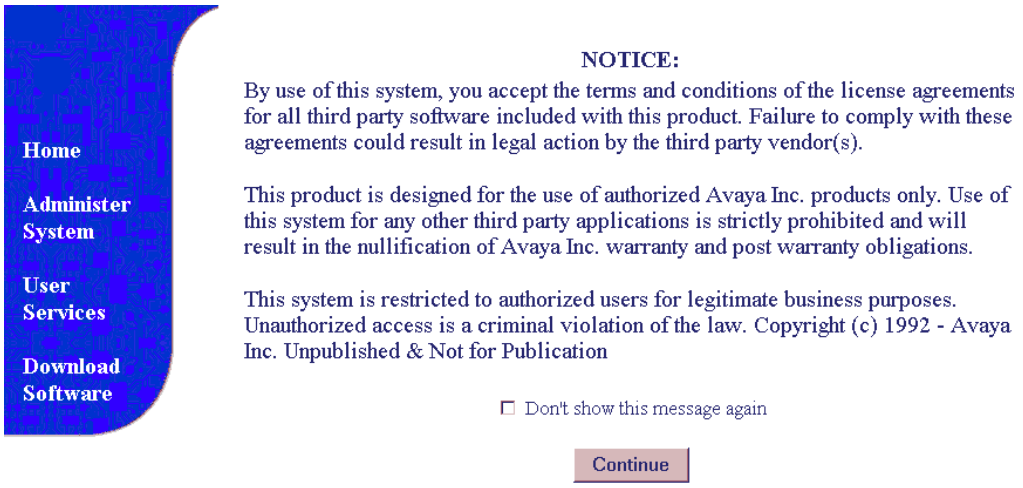
   The S8100 Home page displays:

3. Click **Administer System**.

4 Enter your login ID and password.

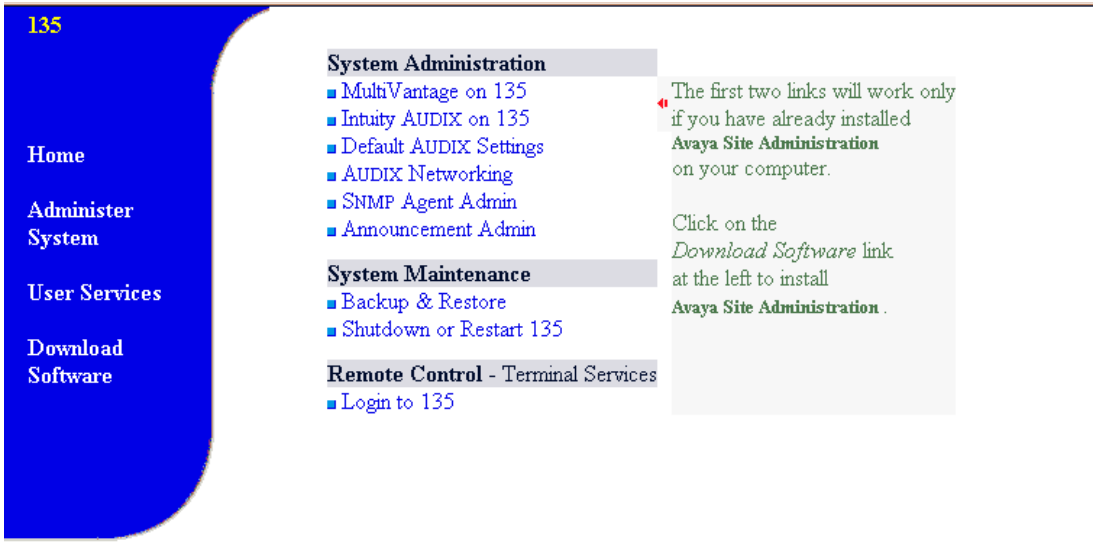
The login ID must have the correct backup permissions and be a member of the S8100 **Administrator's** login group.

The following Notice screen displays:

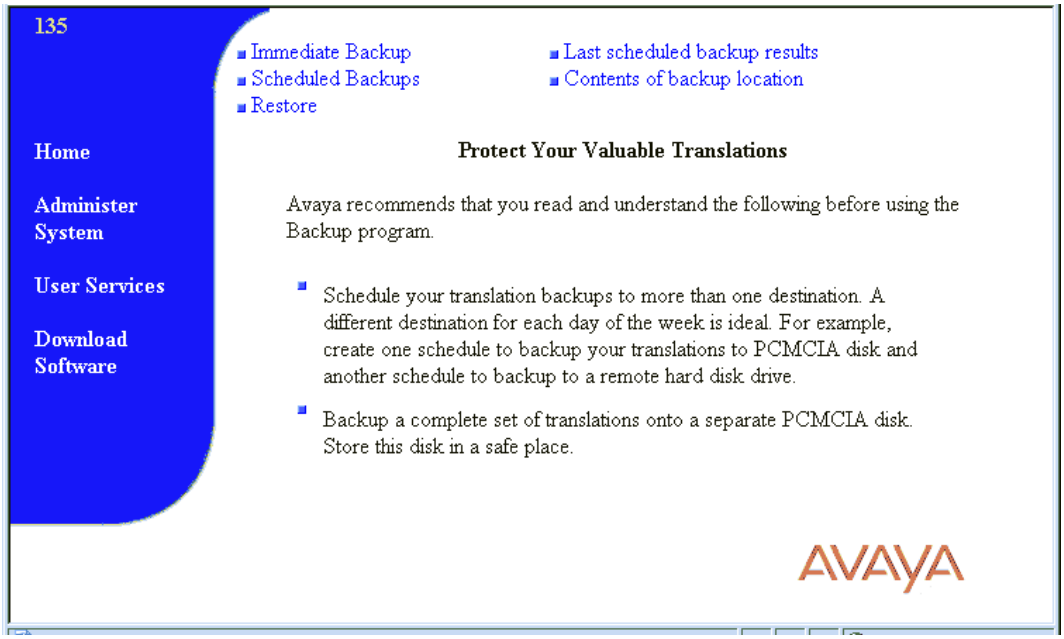


5 Click **Continue**.

The following screen displays:



6 Click Backup and Restore to open the main backup menu.



From the backup and restore main menu, you can:

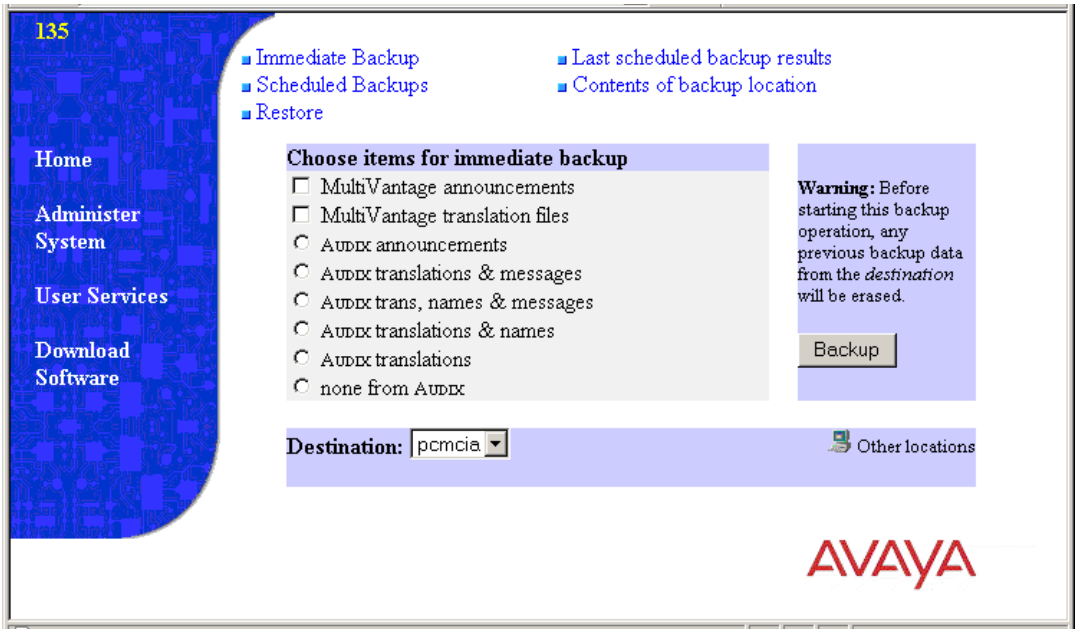
- Perform immediate backups
- Schedule backups (see Schedule backups on page 205)
- Restore backups
- Access last scheduled backup information
- View contents of backup location

NOTE:
As you navigate the backup and restore screens, the main menu items remain available. Use the **Back** button to return to previous screens.

Perform immediate backup

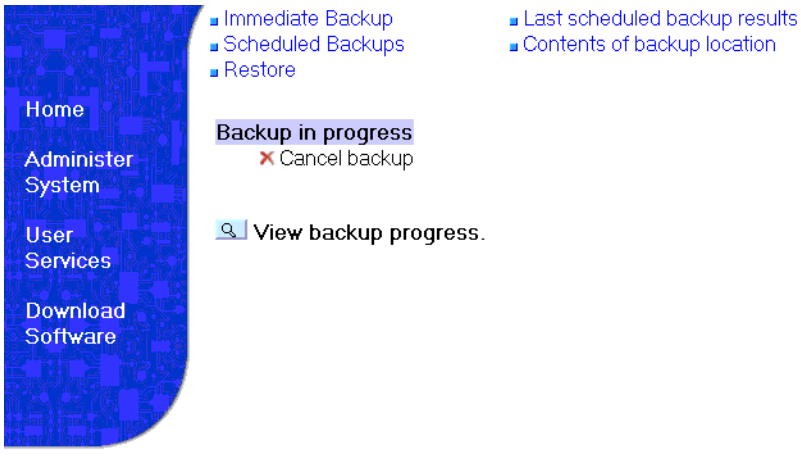
To perform an immediate backup, click **Immediate Backup**.

The following screen displays:



1. From the **Destination** pull-down menu, select a backup destination.This can be a LAN address or a PCMCIA Flash Disk. For this example, select **pcmcia**.
2. Select items for immediate backup.
3. Click **Backup**.

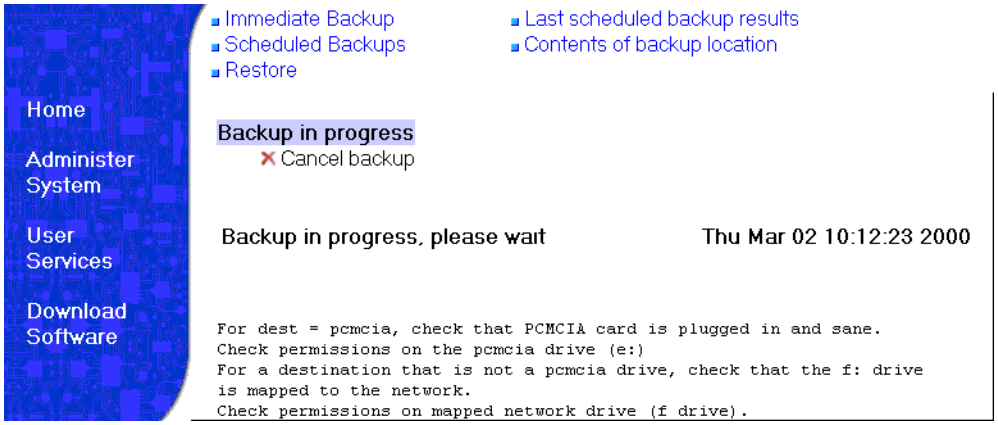
   After you click **Backup**, the following screen displays:



View backup progress

To view backup progress, click **View Backup Progress**.

The following screen displays:

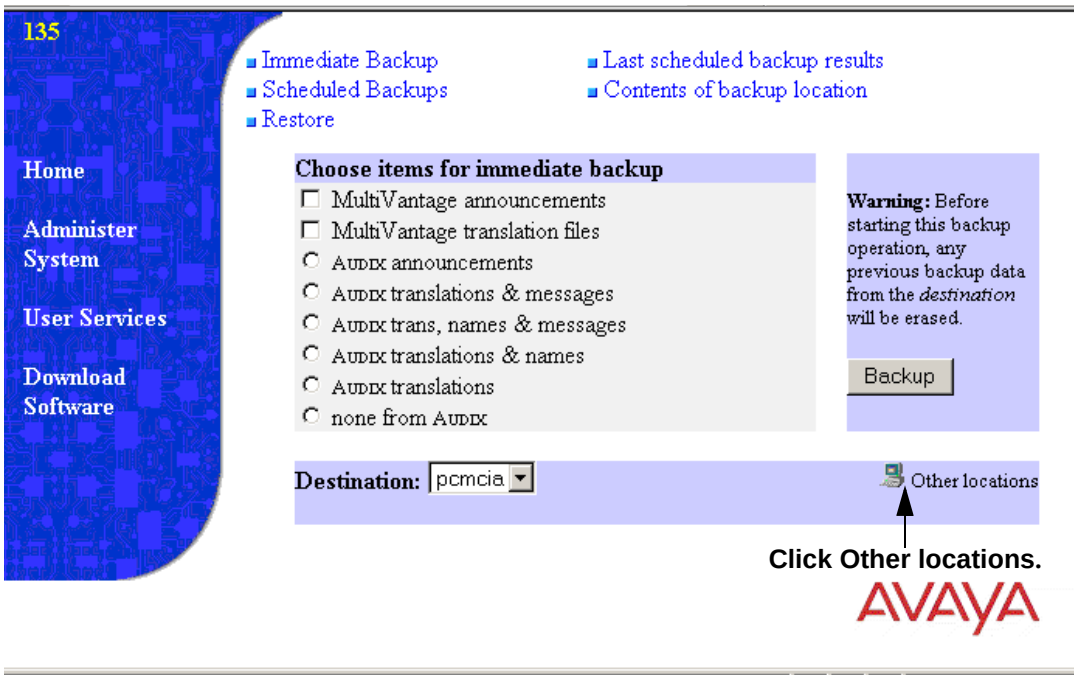


Back up to a LAN address

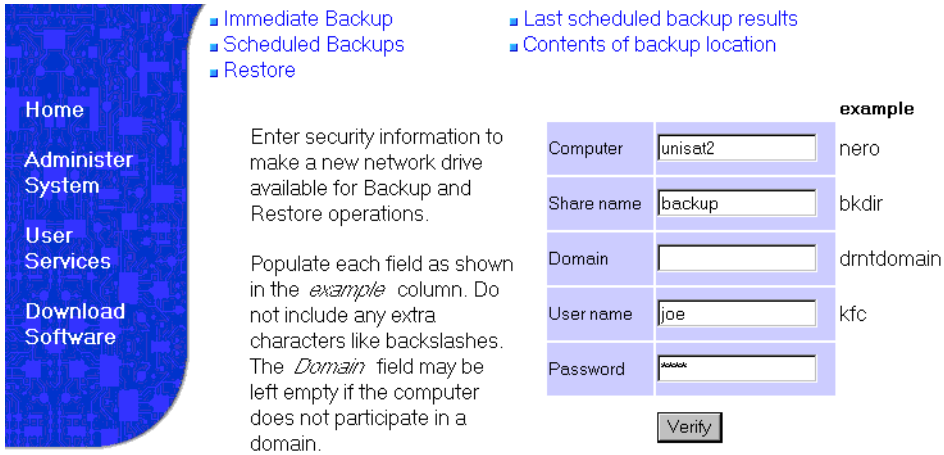
NOTE:
When backing up to a LAN address, the address is to a shared drive that is installed on a non-S8100 machine.

To back up data to a LAN address:

1 Click **Other locations**



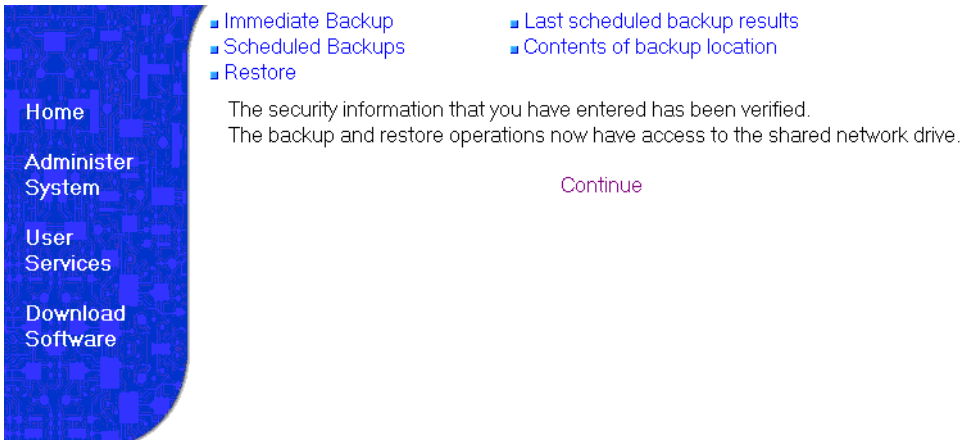
The following screen displays:



2 Enter LAN location information.

3 Click **Verify**.

The following screen displays:



4 Click **Continue** to return to the Immediate backup screen.

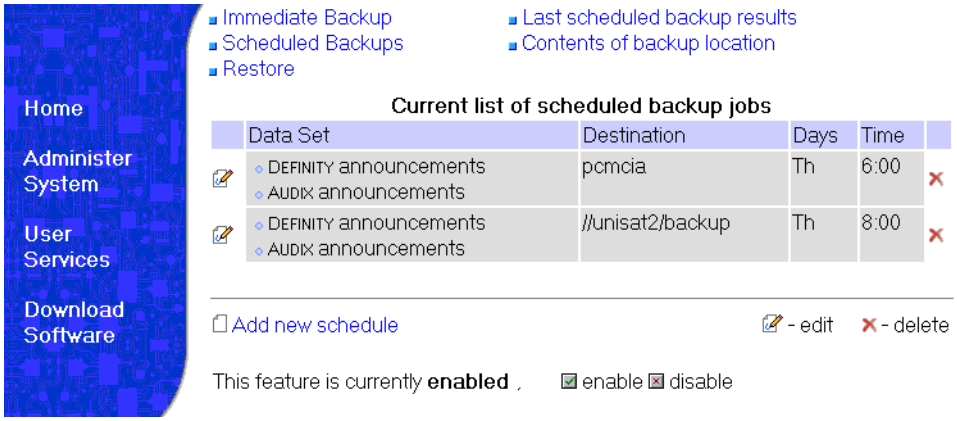
5 Select items to back up and select **Backup**.

View scheduled backups

To view scheduled backups:

1 Click **Scheduled Backups**.

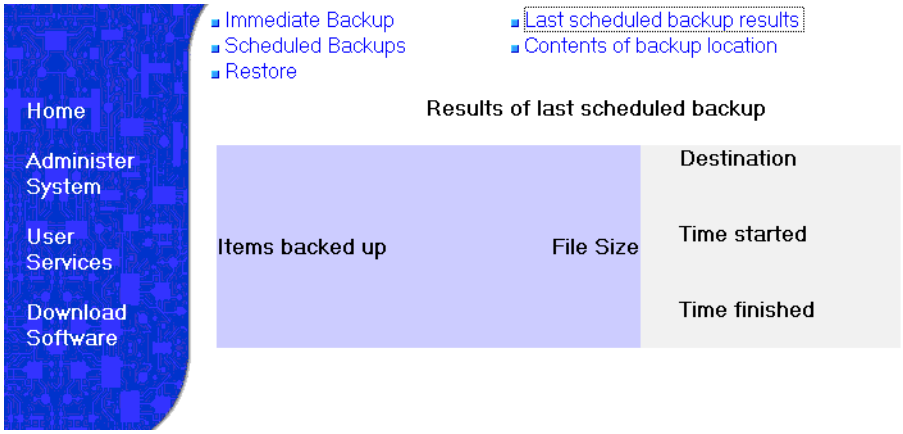
The following screen displays:



From this screen, you can add, edit, or delete scheduled backups. For information about adding a scheduled backup, see Add a scheduled backup on page 205.

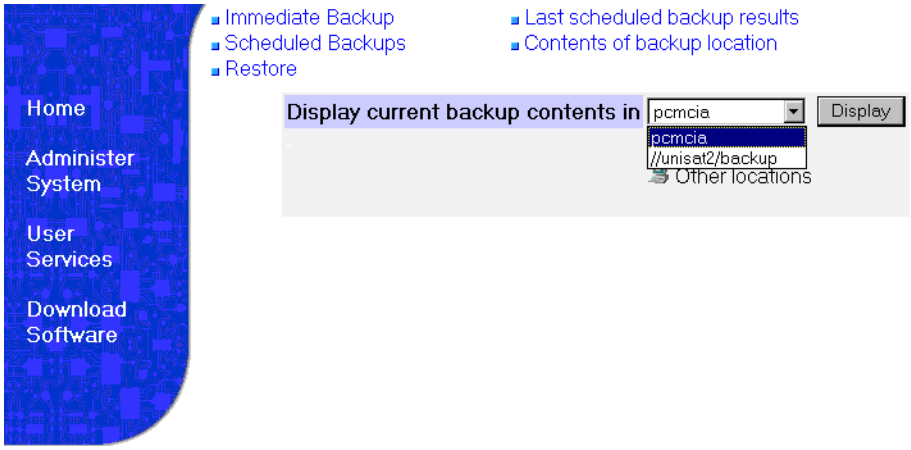
Access backup information

To review previous backups, click **Last scheduled backup results**. The following screen displays:



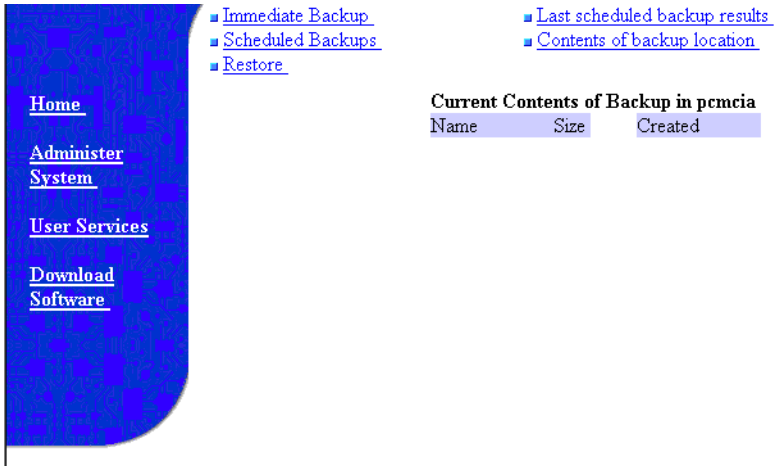
To view contents click **Contents of backup location**.

The following screen displays:



Scroll to the location of backup contents and click **Display** or click **Other locations**.

The following screen displays:

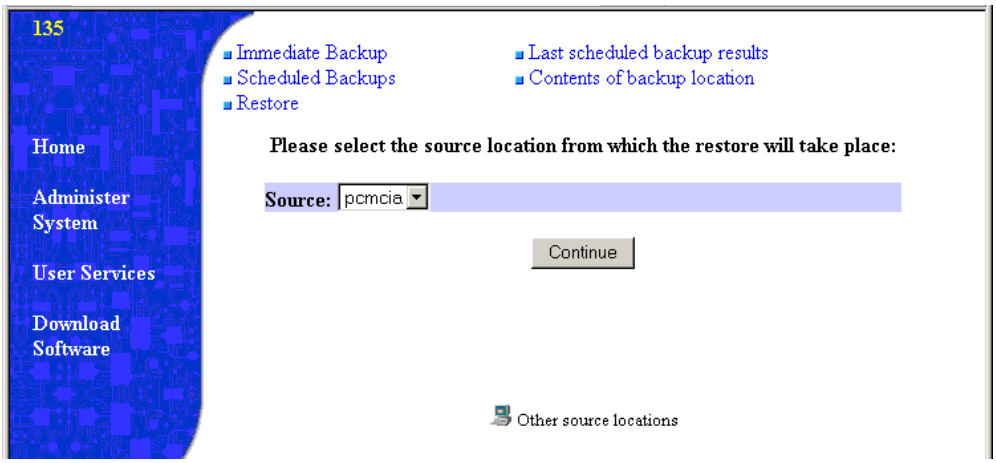


NOTE:
The backup feature can be disabled and later enabled to allow you to perform another function. If disabled, the current schedules remain intact.

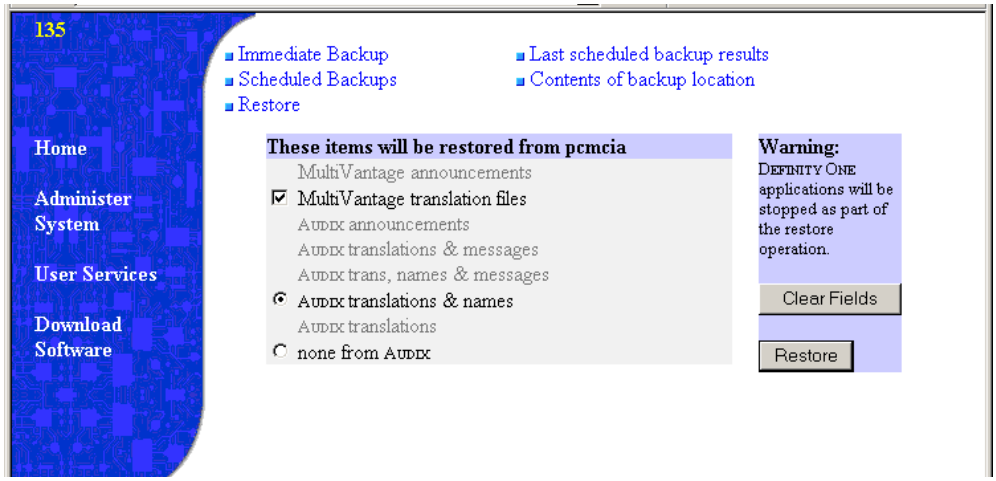
Perform restore

1 Click **Restore**.

The following screen displays:



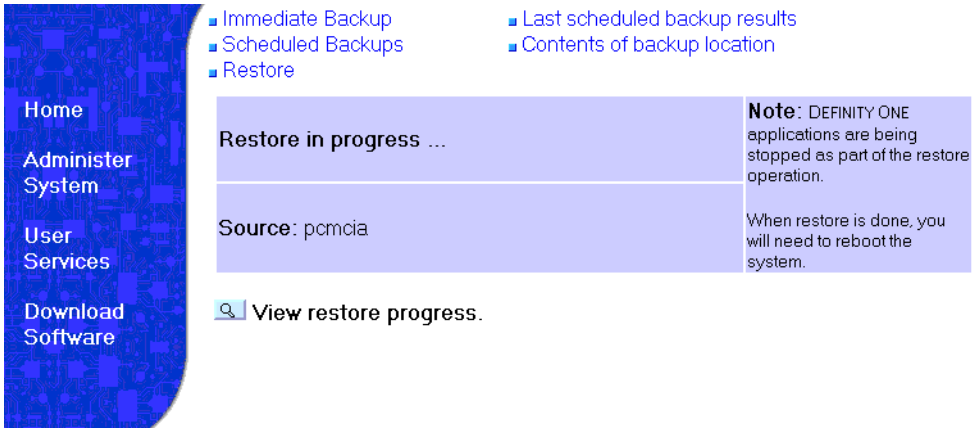
2 Select the restore source and click continue.



3 Select items to restore.

4 Click **Restore**.

The following screen displays:



5 After the restore finishes, reboot the system.

NOTE:
A reboot is required. The restored translations will not be used if the S8100 is not rebooted.

Enable/disable embedded messaging

S8100 supports the capability to disable and enable the embedded INTUITY AUDIX messaging system. Configured from the administration web pages, a disable/enable link allows the user to toggle between active/inactive on-board messaging capability. When the embedded message is active, a ‘disable messaging’ link is present. When the embedded messaging in inactive, the ‘enable messaging’ link is present, and every web page’s reference to INTUITY AUDIX messaging is removed. In the active messaging state, the appropriate backup-restore pages display the various INTUITY AUDIX backup options, whereas in the inactive messaging state, the web pages are modified to not display the message-related backup options.

Impact on maintenance

When INTUITY AUDIX is disabled on the system, the ports on the CWY1 board become unavailable. As a result, maintenance is disabled for the CWY1 board. To counteract this and enable maintenance for the CWY1 board, at least one port on the board must be administered.

Perform the following steps to enable maintenance for the CWY1 board when INTUITY AUDIX is disabled:

1 Add a station using the next available extension:

(For example, if using the Avaya Site Administration tool, click **Add station**, and click **Next**.

2 Enter **1A1201** in the *Port* field.

3 Enter **2500** in the *Type* field.

4 Enter **CWY1 Test Port** in the *Name* field.

5 Submit the form.

6 Perform a **test port 1A1201** command, and verify that the test passes.

Access Diskeeper software to defragment the disk

NOTE:
Do not schedule defragmentation to occur during scheduled maintenance. Open a SAT session and type **display system-parameters maintenance** and press Enter. Note the scheduled maintenance times.

Diskeeper software automatically defragments the disk. The C drive is defragmented once every Sunday at 3:00 a.m., and the D drive once every day between 2:00 a.m. and 4:00 a.m. You can change these times.

Change the default times on Diskeeper

1. From the S8100 desktop, click **Start** → **Programs** → **Executive Software Diskeeper**.

   The Diskeeper menu displays.
2. Select **Action** → **Set It and Forget It**.
3. Select **Partition Scheduler**.
4. Select **Set It and Forget It – Partition Scheduling** window displays.
5. Set new times for automatic defragging. This changes the default times.
6. Click **Start**.
7. Click **Close**.

Access Diskeeper software to defragment the disk

D Recovery

This chapter provides information about system recovery for S8100. This chapter is organized as follows:

- S8100 system-level shutdown and restart on page 317
- Communication Manager software reset (recovery) on page 319
- Reset System 1 (Communication Manager warm start) on page 320
- Reset System 2 (Communication Manager cold start) on page 320
- Reset System 3 (Communication Manager reboot) on page 320
- Reset System 4 (Communication Manager reboot) on page 320
- Reset System 5 (system reboot)

When the system is initially powered up, or when an existing system experiences a catastrophic fault that interrupts its basic functions, the system reboots.

S8100 system-level shutdown and restart

Table 52, Shutdown and restart actions, on page 317 presents system-level shutdown and restart actions that can be initiated by the system technician, the customer, and by hardware. The state of the shutdown and restart actions is indicated by the state of the LEDs on the TN2314 Processor circuit pack (See Appendix E, “LED boot sequence/ TN2314 Processor”). More details about the use of the user commands can be found in *Maintenance for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways* (555-233-149).

Table 52: Shutdown and restart actions ***1 of 3***

Action	Entry	Originated by	Action	Notes
“reboot nice” [campon]	command-line entry from a bash session	technician	Shuts down every application with campon to wait for INTUITY AUDIX users to logoff. The system restarts automatically.	Used for a system reboot after changing a Windows 2000 level parameter that requires a system reboot. This may take an unacceptably long time due to campon of INTUITY AUDIX logons.
“reboot immediate”	command-line entry from a bash session	technician	Shuts down every application without waiting for INTUITY AUDIX users to log off. The system restarts automatically.	Used for a system reboot with a guaranteed reboot time of a few minutes. This action does not wait for INTUITY AUDIX users to be logged off from INTUITY AUDIX.

1 of 3

Table 52: Shutdown and restart actions ***2 of 3***

Action	Entry	Originated by	Action	Notes
"shutdown all" [campon]	command-line entry from a bash session	technician	Shuts down application software while leaving Windows 2000 up. An optional "campon" option may be used to wait for INTUITY AUDIX users to log off.	Used for system upgrade. The campon option may cause an unacceptable wait time. The "start all" command can be used to restart the application software.
"shutdown Audix" [campon]	command-line entry from a bash session	technician	Shuts down INTUITY AUDIX while leaving Communication Manager and Windows 2000 up. An optional "campon" option may be used to wait for INTUITY AUDIX users to log off.	Used to shut down INTUITY AUDIX if the machine name is changed. The "start Audix" command can be used to restart INTUITY AUDIX. The campon option may cause an unacceptable wait time.
"shutdown system" [campon]	command-line entry from a bash session	technician	Shuts down the system without restarting it An optional "campon" options may by used to wait for INTUITY AUDIX users to log off. The system does not restart automatically.	Used to shut down the system in preparation for removing AC power or removing the TN2314 Processor circuit pack. The campon option may cause an unacceptable wait time.The system can be restarted only by removing and restoring power or reseating the TN2314.
"delayed shutdown" button	Web page from a web browser	technician/ customer	Wait for INTUITY AUDIX users to log of f before starting a system shutdown. Depending on a "restart" option, the system may restart automatically.	Used to shut down the system in preparation for removing AC power or removing the TN2314 Processor circuit pack
"immediate shutdown" button	Web page from a web browser	technician/ customer	Do not wait for INTUITY AUDIX users to log off before starting a system shutdown. Depending on a "restart" option, the system may restart automatically.	Used to shut down the system in preparation for removing AC power or removing the TN2314 Processor circuit pack

2 of 3

Table 52: Shutdown and restart actions ***3 of 3***

Action	Entry	Originated by	Action	Notes
Shut-down switch on the TN2314 Processor board's faceplate	Faceplate of the TN2314 Processor board	technician/ customer	Shut down the system after closing every application. The system does not restart automatically.	Used to shut down the system in preparation for removing AC power or removing the TN2314 Processor circuit pack. The system can be restarted only by removing and restoring power or reseating the TN2314.
Detection of the loss of AC power by the UPS	Wiring from the UPS Z3A2 alarm adapter to the Major Alarm lead on the TN2314	Loss of AC power for more than 1 minute	Shut down the system after closing every application. The system restarts automatically upon restoration of AC power.	Provides a graceful shutdown when AC power is lost for more than 1 minute.

3 of 3

Communication Manager software reset (recovery)

There are severe reset levels available to restart Communication Manager. These resets can be user initiated with the **reset system *n*** command (where *n* is the reset level). They may also be automatically initiated by the system's software in response to certain error conditions.

A system is reset due to a loss of power, or through:

- Reset commands entered during a SAT terminal session.
- Maintenance software, from which the system can reset itself. (This process starts when certain software and hardware errors are detected by the software.)

CAUTION:
When the system is rebooted or reset at level 2, 3, 4, or 5, every voice terminal and attendant console feature is adversely affected. Users should be advised of services that are lost and that, as a result, must be reactivated.

The SAT display and circuit pack LEDs indicate the progress of the recovery process.

Reset System 1 (Communication Manager warm start)

- This recovery takes about 60 seconds.
- All software is reset.
- Every stable phone call remains up.
- In-progress calls are dropped.
- No new calls can be made during this time.

Reset System 2 (Communication Manager cold start)

The following are reset:

- All software
- TDM bus
- Every port circuit pack

Every telephone session is dropped. Telephones begin to reconnect to the switch within 60 seconds.

Reset System 3 (Communication Manager reboot)

This is the same as the following Reset System 4. This command is retained for consistency with other Avaya products.

Reset System 4 (Communication Manager reboot)

- Emergency Transfer is invoked in this reset.
- System processes are reloaded from hard disk into memory.
- Every port circuit pack is reset.
- Every telephone session is dropped.

Telephones begin to reconnect to the switch within 60 seconds.

Reset System 5 (system reboot)

This is the same as Reset System 4 (see above).

E LED boot sequence/ TN2314 Processor

This chapter provides information about the LED boot sequence of the TN2314 circuit pack.

This chapter is organized as follows:

- LED boot sequence on page 321
- TN2314 Processor circuit pack on page 321
- TN2314 Processor circuit pack's LEDs (after booting) on page 322
- Table , LED states, on page 324

LED boot sequence

The following describes the LED boot sequence:

TN2314 Processor circuit pack

When power is first applied to S8100, or when the system reboots, the LEDs on the TN2314 circuit pack will light according to this sequence:

1. Every light on the TN2314 blinks in sequence (scrolls), from bottom to top. (The scrolling speed fluctuates, depending on which test is being run.)
2. The 1st and 2nd tests run very fast. – The LEDs scroll quickly.
3. The 3rd and 4th tests run very slowly. – The LEDs scroll more slowly during these tests.
4. The LEDs scroll 17 times during the core testing phase.
5. All three LEDs double-blink when the tests finish.

Any other LEDs that are illuminated indicate an alarm or problem with S8100. For more information about alarms, see Chapter 6, S8100 Windows 2000 Log Events and Alarms in *Maintenance for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways* (555-233-149).

The emergency transfer LED is on if a reset 4 occurs or if power is cycled.

TN2314 Processor circuit pack's LEDs (after booting)

The front panel has 2 groups of LEDs. One group indicates the status of the pack, and the other group (which includes the Major, Minor, and Warning alarms) reflects maintenance conditions in the entire system.

- Red (alarm) – The system has detected a fault in this circuit pack.

  NOTE:
  Alarms on the PROCR, PR-MAINT, SW-CTL, and PKT-INT maintenance objects are indicated by the red LED on the Processor circuit pack.

- Green (test) – The system is running tests on this circuit pack.
- Amber – In an operating system, this LED indicates that the handshaking between the firmware and the Windows 2000 operating system is occurring by flashing briefly once every 10 seconds.
- PCMCIA (amber) – The flash disk is in use
- MAJOR ALARMS (red)
- MINOR ALARMS (red)
- CLOCK (amber) – Blinks once every 4 seconds.
- EM XFER (red) – Indicates emergency transfer has been invoked

  NOTE:
  If the AC power cord is unplugged, the emergency transfer feature invokes, however the EMERGENCY TRANSFER LED (red) is not lit due to loss of AC power. The system gracefully shuts down in about 3 minutes.

- OK REMOVE (green) – Steady indicates that it is OK to remove the TN2314 Processor circuit pack.

WARNING:
DO NOT REMOVE the TN2314 circuit pack unless the green ***Complete Shutdown*** LED is lit. Failure to heed this warning may result in loss of data and/or damage to equipment.

Figure 52: TN2314 circuit pack's faceplate

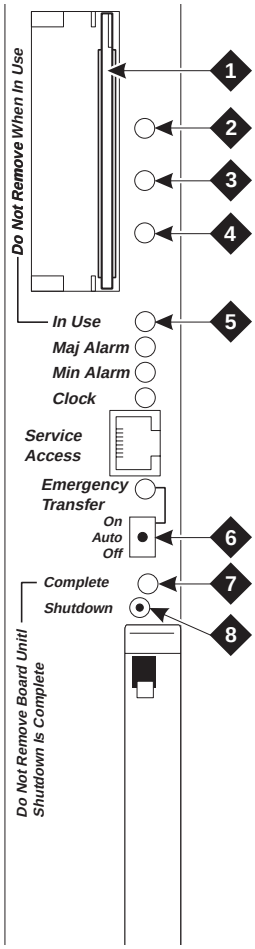


Figure notes

1	PCMCIA slots	**5**	PCMCIA in-use LED
2	Red LED	**6**	Emergency Transfer On/Auto/Off switch
3	Green LED	**7**	Complete Shutdown LED – Safe to pull board when green LED is on steady
4	Amber LED	**8**	Shut-down switch – Gracefully shuts down system

LED states

Table 53, TN2314 circuit pack's LED states, on page 324 summarizes the TN2314 circuit pack LED states.

Table 53: TN2314 circuit pack's LED states

		Boot sequence = 3 min, 45 sec								Shut-down sequence		Other	
LED name	**LED color**	**Power-on reset**	**860 core test in progress**	**860 core test finished, RM initialized**	**PC BIOS boot**	**PC OS boot**	**Firmware download**	**Jump to application firmware**	**SPE up**	**Shutdown in progress**	**Shutdown complete**	**860 core test failed**	**Pentium BIOS update**
TN2314 CP A alarm	red	on	on	Racing LEDs	on	on	on	Racing LEDs	sw	on	on	on	on
TN2314 test	green	off	on		flash1	flash3	off		sw	sw	off	on	flash2
TN2314 in use	yellow	off	off		off	off	flash2		flash 4	sw	off	on	flash2
PCMCIA	yellow	on	on		sw	sw	sw		sw	sw	on	off	on
Major alarm	red	off	off		off	off	off		sw	sw	off	off	off
Minor alarm	red	off	off		off	off	off		sw	sw	off	off	off
Clock status	yellow	off	off		off	off	off		clk	clk	off	off	off
ETR	red	on	on		on	on	on		sw	sw	on	on	on
OK to remove	green	off	on		on	off	off		off	flash3	on	on	off
_____	_____	____	(a)__ 40 sec		(b) 40 sec	(c) 80 sec	(d) 30 sec	(e)					

flash1 – 800 ms ON, 200 ms OFF
flash2 – 500 ms ON, 500 ms OFF
flash3 – 200 ms ON, 800 ms OFF
flash4 – 200 ms OFF on every sanity heartbeat
flash5 – 1 sec ON, 1 sec OFF
sw – Software-controlled
clk – Similar to the TN2182 Tone/Clock LED

F Status LEDs

This chapter provides information about the status LEDs for S8100.

This chapter is organized as follows:

- Attendant console's LEDs on page 325
- Other circuit packs on page 325
- Circuit packs' status LEDs on page 325
- Power supply's LEDs on page 327

Attendant console's LEDs

The console has 2 red LEDs, labeled ALM and ACK. The left LED lights steadily when there is a Major or Minor alarm at the switch cabinet. The right LED lights steadily if the alarm has been successfully reported to INADS. If the system is unable to report the alarm to INADS, the LED flashes, thus signaling the attendant to call INADS and report the alarm. The system calls INADS automatically if it uses a modem.

Other circuit packs

Upon power up, some LEDs may be lit on the other circuit packs. Under normal operation, LEDs on these circuit packs should not light, with the following exception – a solid green LED on any circuit pack indicates that diagnostic tests are being executed on that circuit pack.

Circuit packs' status LEDs

Each circuit pack has 3 LEDs on the front panel visible at the front of the carrier. On every circuit pack, except the 650A power unit, the LEDs indicate:

- Red (alarm) – If the circuit pack is communicating with the system, the system has detected a fault in this circuit pack. An on-board alarm for this circuit pack is displayed in the Alarm Log.

  The circuit pack also lights this LED when either the circuit pack has not yet initialized communication with the system or when the circuit pack loses contact with the system and stops functioning (circuit pack is said to be "in reset"). In these cases, there may not be an alarm in the Alarm Log. To determine if the red LED is lit because the circuit pack is not in contact with the system, issue the **list configuration board PCSS** command, where PCSS refers to the slot containing this circuit pack. If the system does not detect the circuit pack, this command returns **Identifier not assigned or no board**.

If the circuit pack has just been inserted, the system may still be initializing the circuit pack. If, after 5 minutes, the circuit pack still has not initialized communications with the system, check the MO for any special instructions. If the MO does not provide the needed information, perform the following steps:

1. Check the Error Log for TONE-BD and TDM-BUS errors. Follow appropriate sections for any TONE-BD and TDM-BUS errors.
2. Reseat the suspected circuit pack.

WARNING:
Reseating a TN2314 can be very destructive. This should be done only if its green Complete Shutdown LED is lit. Otherwise, you must shut down before reseating.

3. Wait 5 minutes. Then issue the **list configuration board PCSS** command. If the result indicates that the system still has not registered the circuit pack, go to next step.
4. If the system seems to be functioning correctly, but the circuit pack does not start communicating with the system, replace the circuit pack.

- Green (test) – the system is running tests on this circuit pack.
- Yellow (busy) – indicates that the circuit pack is in use.

NOTE:
A port circuit pack also lights its red LED when it performs initialization tests (for example, when the circuit pack is initially inserted into the system). If every initialization test passes, the red LED is turned off. If not, the red LED remains lighted and the circuit pack is not placed into service.

During the various states of operation (start-up testing, normal operation, circuit failure, and so forth) circuit pack status LED indications appear as shown in Table 54, Control and port circuit pack status LEDs, on page 326.

Table 54: Control and port circuit pack status LEDs

Equipment type	LED	Description
Port circuit packs	Red	***Briefly on*** during a power up, a circuit pack's reseating or resetting, or system reset. ***Steadily on*** if a circuit pack fails start-up test or fails while in use. ***Off*** during normal operation.
	Green	***Briefly on*** during a circuit pack's testing following power up, a circuit pack's reseating, or a system reset. ***On*** during periodic, scheduled, or a technician's on-demand testing. ***Off*** during normal operation.
	Yellow	***On*** when any of a circuit pack's ports are in use (otherwise, ***off***).

Power supply's LEDs

Table 55, LED and alarm conditions, on page 327 shows the LED and alarm conditions for the 650A power supply. Ring voltage and neon bus output do not activate alarm status.

Table 55: LED and alarm conditions

Condition	LED status	Alarm state
Normal	Red off; Yellow on	Open
No input power	Red off; Yellow off	Closed
DC output not present (except Neon)	Red on; Yellow off	Closed
Fan alarm	Red on; Yellow on	Closed

G GAS commands in bash

This chapter provides information about bash commands that are used in the installation process. It also includes information about the **setip** command. These commands are not available to the customer.

Avaya (Lucent) access controller bash commands

The following commands are useful during installation and maintenance tasks and are allowed for the avaya logins. After opening the LAC bash shell, enter the name of the command. Refer to *Maintenance for the Avaya S8100 Media Server with the Avaya G600 and CMC1 Media Gateways*, 555-233-149 for detailed information.

Table 56: Bash commands for Avaya logins ***1 of 3***

Command	Description
alarmorig	Turns on alarm origination from the GAM (INADS)
alarmstat	Gives global alarm status (major, minor, or none) for the GAM, Communication Manager, and INTUITY AUDIX
autobackup	Enables and disables backup commands
cleargamalarm	Clears every GAM alarm after failure conditions are repaired
d1backup	Backs up translations and other data to the specified destination
d1disable SNMP	Disables SNMP
d1enable SNMP	Enables SNMP
avaya help	Displays help for every available command
d1restore	Restores data (from a specified source) that was backed up with the d1backup command
downloadboot	Enables download of boot image to firmware
identbackup	Identifies the data (on a specified source) backed up with the d1backup command

1 of 3

Table 56: Bash commands for Avaya logins ***2 of 3***

Command	Description
environment	Displays the TN2314 temperature and voltage ranges
ftpserv	Enables the FTP service
fileversion	Queries Windows 2000 for executable file
fwversion	Displays command version number
gamalarmstat	Displays GAM alarm information formatted as follows: mm/dd/yyyy = month/day/year Windows 2000 Event Log Name= System | Security | Application Alarm Source= Windows 2000| GAM | LAC | GSK | VFM | GAS Windows 2000 Event Type = Error | Warn | Info Alarm Type = Major | Minor Event ID= Event field in Windows 2000 Event Log ACKed= ACKed, NACKED, FAILURE, NO_OSS_RESPONSE
net user	Used to add/activate logins, change passwords
oss	Sets telephone numbers for outgoing INADS calls
post	If no argument is given, postcodes are sent to the 860 firmware with the results sent to standard output.
rasdrop	If no argument is given, rasdrop schedules the RAS service to stop and restart in 2 minutes from when it was run.
reboot	Reboots system as follows: **nice**: Shuts down applications and Windows 2000 in a graceful manner **immediate**: Reboots the system without waiting for the applications to shut down, causing possible loss of voice messages that are being recorded and every call to drop
restartcause	Displays the restart causes for system (for technician/TSC)
serialnumber	Reads and displays the serial number of the circuit pack
setip	Sets the IP address, subnet mask, and default gateway of the LAN interface to the customer's LAN (out the splitter cable). Turns on RAS. Reboot is required for this to take effect.

2 of 3

Table 56: Bash commands for Avaya logins ***3 of 3***

Command	Description
shutdown	Shuts down: **all** – Every Avaya S8100 application **system** – Every Avaya S8100 application and Windows 2000 **appname** – AUDIX (for example, shutdown Audix) **camp-on** (optional INTUITY AUDIX feature) – Notifies users of an impending system shutdown and waits for users to end their sessions before shutting down.
start	Called from a bash shell on S8100 to start an application through Watchdog
statapp	Displays the status of every application group running on the system. Displays the current status of each application. Applications states are: Up, Down, or Partially Up. Displays every process associated with an application regardless of its state.
swversion	Lists the version of software running on S8100
terminate	Called from a bash shell on S8100 to terminate applications
versiondiff	Compares Windows 2000 executables against version entered at the command line
vilog	Merges and displays the various log files in the system

3 of 3

LAC commands

Table 57: LAC commands

Command	Description
AUDIX	Connects to INTUITY AUDIX SAT
bash	Invokes the bash shell. The bash shell has useful commands for administration and installation.
multivantage	Connects to SAT
cmd	Brings up a DOS prompt
exit	Exits the bash shell
loadlicense	Installs the license file
loadpwd	Sets passwords for Windows 2000 Administrator and Guest logins (admin, user)

setip command

Use the **setip** command from a LAC bash shell to set certain Windows 2000 specific settings. To get to a bash shell:

1. Telnet to the S8100 over any interface.
2. Login.
3. Enter **bash** at the LAC prompt.

Once you are in a LAC bash shell you can run **setip**.

NOTE:
Setip settings require a reboot before taking effect. Set every necessary parameter before issuing the reboot command.

Display current settings

To display current settings, run **setip** with no parameters.

Setip allows setting the customer's LAN address along with subnet mask, gateway, DNS and WINS settings. It also allows setting the machine name and the RAS IP addresses.

Set the machine name in Windows

To set the machine name:

1. In a bash shell, type **setip name=machineName**. Limit the machine name to 10 characters. Setip allows you to enter more characters; however INTUITY AUDIX only displays the first 10 characters of the machine name in its administration window.

   Example:**setip name=mysite**

NOTE:
After having set the machine name, the **setip** command displays the new settings and the old settings.

NOTE:
You will also need to set the host name. See Set DNS addresses and host name on page 333.

Set RAS IP address

NOTE:
INADS will provide this IP address.

To set the RAS IP address:

1. In a LAC bash shell, type **setip ras=<ip-address>**

   Example: setip ras=10.21.0. 53

NOTE:
This command not only sets the RAS IP address, it also starts the service. Turn off RAS service if system is set up without a modem.

After having set the RAS IP address, the **setip** command displays the new settings and as the old settings.

Set the customer's LAN, DNS, and WINS information

Set LAN address

To set the customer LAN address:

1. Get the IP address of the S8100, subnet mask, and default gateway addresses from the customer.
2. From a LAC bash shell, run the **setip cust=ip-addr,netmask[,gateway]**. The gateway address is optional but the ip-address and subnet mask are required.

Example: setip cust=155.9.162.121,255.255.255.0,155.9.162.2

After setting the customer's IP address, the **setip** command displays the new and the old settings.

Set DNS addresses and host name

If the customer is using DNS you can set DNS information with the **setip dns=name,domain-name,primary-dns-ip-addr[,secondary-dns-ip-address]**, This sets the DNS host name, domain name, and the list of name server IP addresses.

Ex: setip dns=CustomerHost,CustomerDomain.com,155.9.1.10,155.9.15.14

After having set the customer's DNS IP address, the **setip** command displays the old settings as well as the new settings.

Set WINS addresses

If the customer is using WINS you can set WINS information with the **setip wins=[ip-addr-primary[,ip-addr-backup]]**. This will set the IP address of the primary and secondary IP addresses for the windows NetBios on the TCP name server.

Ex: setip wins=155.9.145.1,155.9.145.4

After setting the customer's WINS IP address, the **setip** command displays the new and the old settings.

Once you have set every appropriate settings for your location, enter reboot nice to restart the system with the new settings.

Other commands

ftpserv command

The **ftpserv** command is executed from a console bash shell and turns on the FTP server. If you attempt to ftp into the S8100 and receive a **connection refused** message, then ftp is not running.

To turn on FTP, enter **ftpserv**.

To turn off FTP, enter **ftpserv -c**.

statapp command

The **statapp** command is used from a LAC bash shell to determine the current status of each application.

Table 58: Example: S8100-avaya1>statapp

W2000	12/10	UP
W2000 WEB	1/1	UP
W2000 TERMSERV	1/1	UP
W2000 Console	1/2	in use
CoResServ	5/5	UP
Communication Manager	51/51	UP
SNMP	3/3	UP
CornerStone	4/4	UP
AUDIX	15/33	PARTIALLY UP
AUDIXNet	0/5	DOWN
MISC	24/0	UP

net user commands

The net user commands manipulate Windows 2000 level logins on the S8100 system and can be used to add new logins, change passwords on existing logins, or simply to enable/disable existing Windows 2000 accounts.

To add a new user, execute the following command from a bash shell:

net user username password

To change the password of an existing login, execute the following command from a bash shell:

net user username newpassword

To enable an existing login that is disabled, execute the following command from a bash shell:

net user username /active

H Installation connectivity quick reference

This appendix provides a tear-out quick reference sheet summarizing physical connections, access methods, and login information for S8100.

You can physically connect to an S8100 system in several ways, as described in the following table.

Physical connection	IP address
Local monitor/mouse/keyboard	**127.1**
Laptop PCMCIA network connection	**192.11.13.6**
PC or laptop with RAS modem (dial-up)	**10.21.0.X** (**X** is customer-dependent — Avaya-assigned)
PC or laptop on customer's LAN	Customer-dependent (default login value of **192.11.13.9**)

Once you are physically connected, there are several ways to access S8100, as shown in the next table.

Access method	
Telnet	<**ip addr**> [**Start** → **Run...**]
Avaya Site Administration	**using appropriate ip-addrs**
Web browser	**http://**<**ip-addr**>
Terminal server	**use Terminal Services client**

The following table shows login information for Avaya personnel.

Logins to enter system	Logins to enter Communication Manager	Logins to enter INTUITY AUDIX
lucent1	**dinit**	**atsc**
lucent2	**dinads**	**acraft**
lucent3	**dcraft**	**acraft**

- Each row of logins has the same password. For example, the **lucent1**, **dinit**, and **atsc** logins all have the same password.
- The lucent logins are used to access the web browser and terminal server.
- Every login can be used for Telnet access.
- The **d** and **a** logins (columns 2 and 3) are used for Avaya Site Administration access.

I Map CD-ROM for an S8100 upgrade

This appendix provides the steps to map the S8100's server to your laptop's CD-ROM drive so that the server can copy files from a CD-ROM in the laptop.

Prepare to access the S8100

1 Log into your laptop.

Activate the Guest account

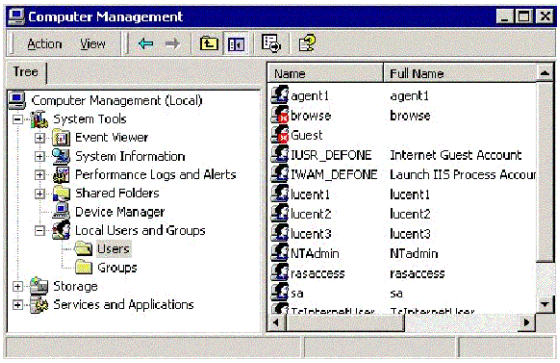
Check the Guest account's current setting

1 At the Windows desktop, right-click the My Computer icon, and select Manage in the help menu.

The Computer Management console displays.

2 Expand "Local Users and Groups" by clicking its "+" sign, and then click the "Users" folder.

NOTE:
A red "X" in the "Guest" user's icon indicates that this user is currently disabled.



Enable the Guest account

1. Click Start → Run, type CMD, and then click OK to open a DOS window.
2. At the CMD prompt, enter the following command:

   ```
   net user guest guest123
   ```

3. Enter the command:

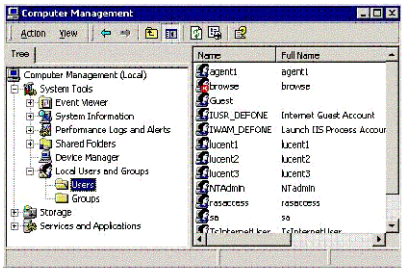
   ```
   net user guest /active
   ```

   NOTE:
   The Guest account should now be enabled.

4. Enter **exit** to close the DOS window.

Verify the Guest account's new setting

1. Return (toggle back to) the Computer Management console.
2. On the toolbar, click the Refresh button (3rd from right) to update the screen's status.



   NOTE:
   The Guest user's icon should ***not*** be marked a red "X".

3. In the Computer Management console's title bar, click the "X" to close the window.

Share the laptop's CD-ROM drive

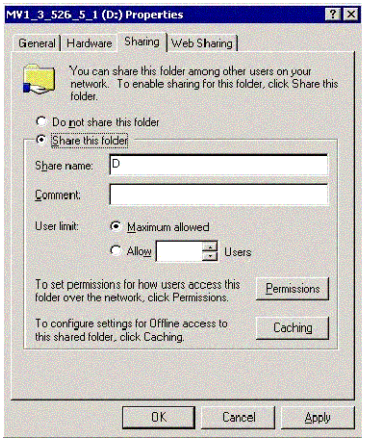
1. At the laptop's Windows desktop, double-click the My Computer icon.

   The My Computer window contains the various laptop's devices.

   NOTE:
   Since, your laptop's CD-ROM drive is normally an unshared device, its icon should ***not*** be marked with a hand.

2. Right-click the CD-ROM device, and select "Sharing…" in the help menu.
3. In the Sharing tab of the Properties dialog:
   a. Click the "Share this Folder" option
   b. If desired, specify the laptop's Share Name (for example, "Laptop CD-ROM".)

   NOTE:
   The following figure shows the CD-ROM's default share name, "D."



4 Click the Apply button to enable your changes.

5 Click OK to close the Properties dialog.

6 At the My Computer window, verify that the CD-ROM device is now marked with a hand.

Connect to and access the S8100

Prepare to access the S8100's desktop

1 If this is an R9.5 S8100 system, use pcAnywhere to access the S8100's Windows desktop. If ***not*** ($R10^{+}$), use Remote Desktop Client.

NOTE:
Whereas, Remote Desktop Client is a free application – pcAnywhere is ***not*** and must be ***preinstalled*** on your laptop.

NOTE:
Avaya does **not** support the Remote Desktop Client application.

2 If necessary, download the current Remote Desktop Client from the following Microsoft link:

http://download.microsoft.com/download/whistler/tools/1.0/wxp/en-us/msrdpcli.exe

Connect to the S8100

1 Directly connect to the S8100's services port. For details, refer to Direct connection to the RJ45 service jack on page 140.

2 Open the laptop's Remote Desktop Client application.

3 In the Remote Desktop Connection dialog, type **192.11.13.6** (as the server's IP address) and then click Connect.

The S8100's Windows application responds with the Log On to Windows dialog.

4 Log into the S8100 with the proper credentials.

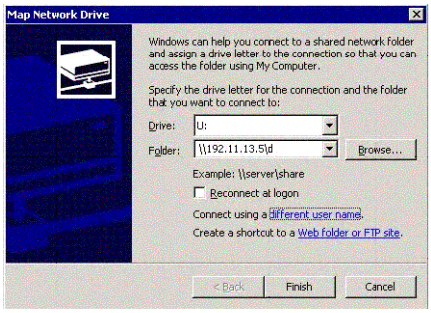
You are now at the S8100's Windows desktop.

Map to the laptop's CD-ROM drive

1 At the S8100's desktop, right-click the My Computer icon, and then select "Map Network Drive…" in the help menu.

This enables the Map Network Drive wizard (see Figure 53, Map Network Drive wizard, on page 342).

Figure 53: Map Network Drive wizard



2 Within this wizard :

a Type an available letter for a logical drive, followed by a colon (for example, "Q:")

b Type the laptop's IP address (that is, **192.11.13.5**) and the shared folder's name (for example, "D" or "Laptop CD-ROM") – in the following format:

`\\192.11.13.5\d`

(**or** `\\192.11.13.5\Laptop CD-ROM`)

c Click (Connect using a) "different user name" to access the "Connect As…" dialog.

Within this dialog, type:

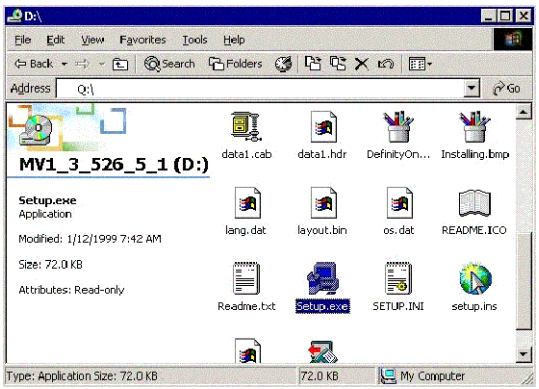
a Type **Guest** as the user name.

b Type **guest123** as the password.

c Click OK to close the dialog.

d Click the Finish button to close the wizard.

The S8100 can access the laptop's shared folder as shown in the following figure.



J Install and cable a CMC1 cabinet

Primarily to assist hardware additions and maintenance activities, this appendix describes procedures for installing and cabling a CMC1 cabinet to physically connect and access the S8100 Media Server with CMC1 Media Gateways.

NOTE:
A CMC1 is a wall- or table-mounted cabinet, whereas G600 is a 19″rack-mounted cabinet. For information about installing a ***G600*** cabinet, see Chapter 1, "Install and cable a G600 cabinet".

NOTE:
The physical installation of a CMC1 cabinet is similar to a ProLogix cabinet. The cabling is also similar, except for the Processor Interface cable (multileg cable). Do not access applications, such as Communication Manager, until installation and cabling of the cabinet are finished. Your configuration can consist of an S8100 Media Server with 1, 2, or 3 CMC1 Media Gateways.

This appendix is organized as follows:

- Check customer's order on page 343
- Correct shipping errors on page 344
- Unpack and inspect on page 344
- Install an S8100 with a CMC1 system cabinet on page 348
- Check AC power and ground for CMC1 on page 357
- Cable a CMC1 system on page 367
- Install CMC1 main distribution frame (MDF) and external modem on page 370
- Install equipment-room hardware for CMC1 on page 372
- Set ringing option for CMC1 on page 385

NOTE:
After installing and cabling an S8100 with a CMC1, see Section II – Install telephones and make auxiliary connections on page 99 of Chapter 1, "Install and cable a G600 cabinet".

Check customer's order

1. Check the customer's order and the shipping packing lists to confirm that all equipment is included.
2. Report missing equipment to an Avaya representative.
3. Check the system adjuncts and report any damage according to local shipping instructions.

Correct shipping errors

1. Red-tag any defective or over-shipped equipment, and return it according to instructions from National Parts.
2. Direct any short-shipped reports to National Parts. Contact the appropriate location for specific instructions. For a streamlined implementation, call 1-800-772-5409.

Unpack and inspect

DANGER:
Use lifting precautions! A fully loaded CMC1 weighs 58 lbs (26.3 kg). If the doors, power unit, and circuit packs are removed, the CMC1 unit weighs only 29 lbs (13.1 kg).

1. Verify the equipment received. See Figure 54, Equipment packed with a single CMC1, on page 345. Actual equipment may vary in appearance and may ship in separate packages. Equipment comcodes are listed in Table 59, Comcodes for equipment used with CMC1, on page 346.
2. Before mounting the cabinet, remove the CMC1 cabinet's doors by opening and then lifting them straight up and off the hinge pins.

Figure 54: Equipment packed with a single CMC1

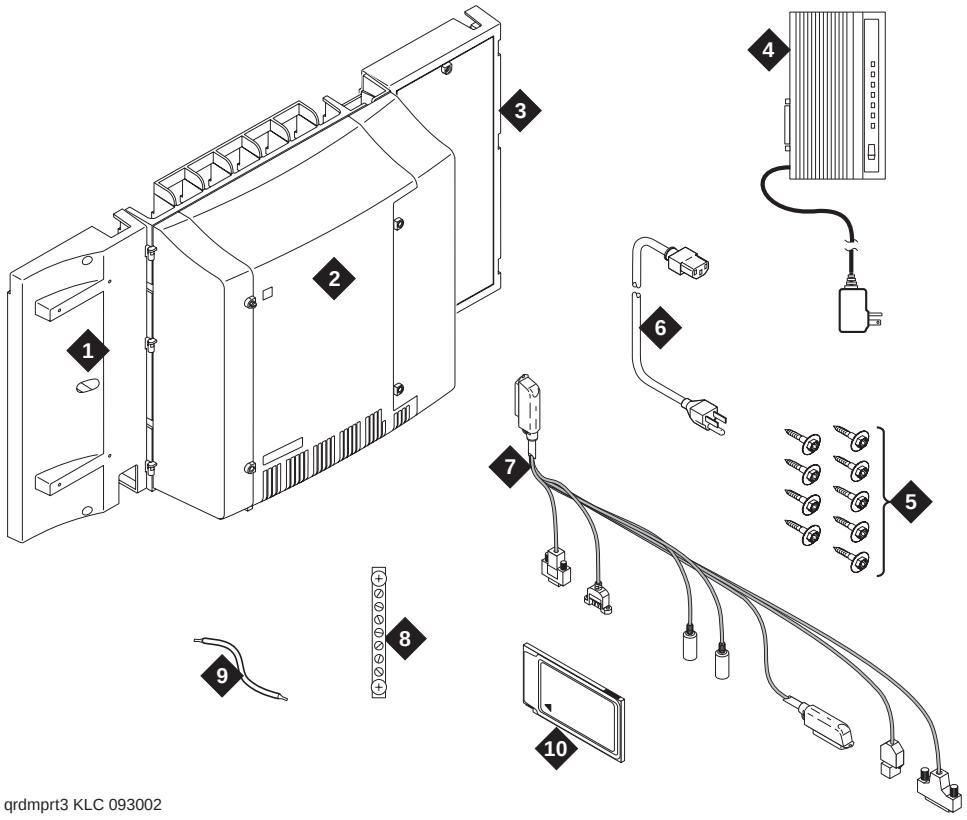


Figure notes

1 Left panel (also acts as wall-mounting template and as floor-mounting pedestal)

2 CMC1 cabinet

3 Right panel

4 External modem (not shipped with every system)

5 #12 × 1-inch shoulder screws

6 AC power cord (NEMA 5-15P or IEC 320)

7 Processor Interface cable

8 Single-point ground block

9 14-inch (35.5-cm) 6 AWG (#40) (16 mm^2) ground wire

10 Flash card (backup)

Table 59, Comcodes for equipment used with CMC1, on page 346 lists the comcodes for equipment used with the CMC1. If “Optional” is marked with an "×", the equipment may be unnecessary, depending on the site’s configuration.

Table 59: Comcodes for equipment used with CMC1 ***1 of 2***

Comcode	Description	Optional
700225758	Left panel	
847951670	Right panel	
700225741	Right panel assembly	
700225360	Right door	
700225766	Left door	
700225782	Fan assembly	
847987187	CMC1 110 cross-connect assembly (main distribution frame) – recommended	×
103970000	Main distribution frame label (Code 220A)	×
407745009	Fan air filter	
706827717	Single-point ground block	
407772888	Time-division multiplexing/local area network (TDM/LAN) bus cable (horizontal)	
407772870	Time-division multiplexing/local area network (TDM/LAN) bus cable (vertical)	
601929763	Processor Interface cable (multileg cable), TN2314	
108549494	TN2314 Processor circuit pack	
848320800	Hard disk programmed	
407633999	US Robotics Sportster external modem	×
601929920	Software CDs	
408166783	PCMCIA flash card (for backup)	
105631527	Time-division multiplexing/local area network (TDM/LAN) bus terminator (AHF110)	
H600-487	14-inch (35.5-cm) 6 AWG (#40) (16 mm^2) green ground wire	
407676691	120-VAC power-distribution unit (145D 6-AC)	×
107949364	650A power supply	
848477634	LAN cross-over cable (RJ45), 12-foot	
405362641	120-VAC power cord	
106278062	Apparatus blank (circuit-pack blank) (158P)	
106606536	Integrated channel-service unit (ICSU) (120A2)	×

1 of 2

Table 59: Comcodes for equipment used with CMC1 ***2 of 2***

Comcode	Description	Optional
107988867	DS1 loop-back jack (T1 Only) (700A)	×
848477634	Cross-over cable	×
107152969	75-Ohm DS1 coaxial adapter (888B)	×
403613003	157B connecting block (“sneak-current protectors”)	×
406948976	6SCP-110 protector	×
107435091	507B sneak-current fuse panel	×
407216316	220029 sneak-current fuse	×
104307327	C6C cable – 50-foot (15.2-m) shielded DS1 cable with 50-pin male to 15-pin male	×
104307376	C6D cable – 50-foot (15.2-m) shielded DS1 cable with 50-pin male on each end	×
104307434	C6E cable – 100-foot (30.5-m) shielded DS1 cable with 50-pin male to 50-pin female	×
104307475	C6F cable – 50-foot (15.2-m) shielded DS1 cable with 50-pin male to 3 inch (7.62-cm) stub	×
102381779	3B1A carbon block	×
104410147	3B1E-W wide-gap gas tube	×
105514756	3C1S analog-line protector – solid state	×
102904893	4B1C carbon block with heat coil	×
104401856	4B1E-W wide-gap gas tube w/heat coil	×
104386545	4C1S analog-line protector – solid state with heat coil	×
105581086	4C3S-75 digital voice-circuit protector – solid state	×
406144907	ITW LINX gas tube, avalanche suppress	×
901007120	ITW Linx ground bar (used with above)	×
406304816	ITW Linx replacement fuse	×
103972758	Data-link protector (1 circuit)	×
103972733	Data-link protector (8 circuits)	×
407063478	Electrostatic discharge (ESD) wrist strap	
107949364	Avaya online 650A UPS	×
407691401	Z3A2 alarm adapter (required with UPS)	×

2 of 2

Install an S8100 with a CMC1 system cabinet

A CMC1 cabinet can be either floor- or wall-mounted. Set the Carrier Address ID installing each CMC1 cabinet.

Verify the carrier address ID on CMC1 cabinets

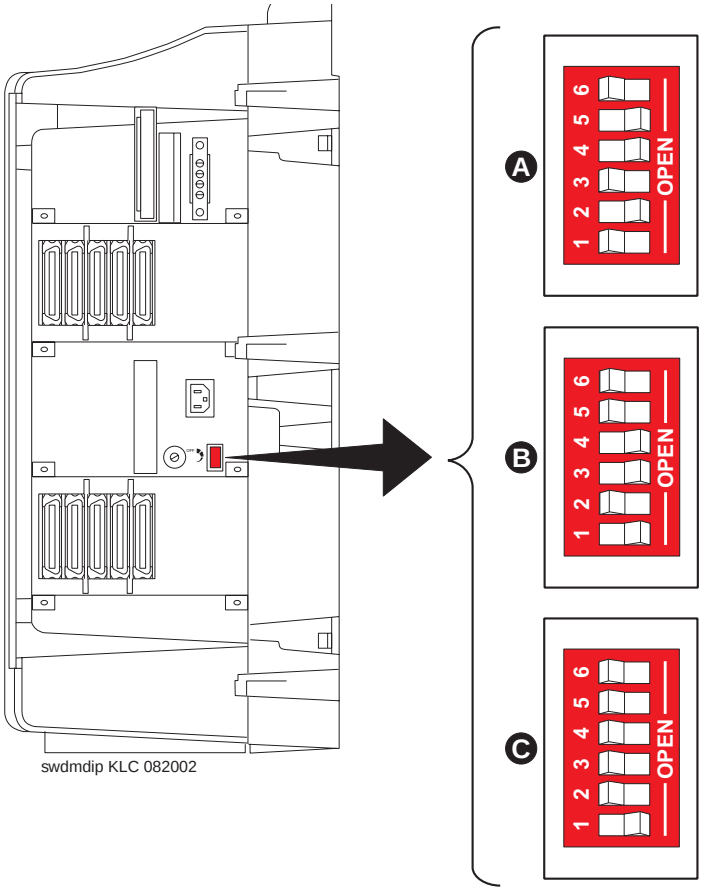
1 Verify and, if necessary, set the carrier address ID for each cabinet as shown in Table 60, Carrier address ID settings, on page 348 and Figure 55, Setting CMC1 carrier address ID (right side), on page 349. Cabinet A is the processor cabinet and cabinets B, C, and D optional port carrier cabinets (S8100 supports up to three cabinets, A, B, and C).

Table 60, Carrier address ID settings, on page 348 shows the settings for cabinets A, B, C, and D. The **1**s and Os indicate closed and open positions, respectively, of the 6 rocker switches on the switch panel. For example, switches 2, 4, and 5 are in the closed position for cabinet A. This table is embossed on the cabinet next the switch panel.

Table 60: Carrier address ID settings

	A	B	C	D
6	O	O	O	O
5	**l**	O	O	**l**
4	**l**	**l**	O	O
3	O	**l**	O	O
2	**l**	O	O	O
1	O	**l**	**l**	**l**

Figure 55: Setting CMC1 carrier address ID (right side)



2 Proceed to either Floor mount the CMC1 cabinet on page 350 or to Wall mount the CMC1 cabinets on page 350.

Floor mount the CMC1 cabinet

The dimensions of each cabinet (with floor pedestal) are 28.5 inches (72.4 cm) high × 24.5 inches (62.2 cm) wide × 12 inches (30.5 cm) deep. Maintain a service clearance of 12 inches (30.5 cm) on the left, right, and front of the cabinet. If your configuration requires 2 cabinets, be sure each maintains the service clearance of 12 inches (30.5 cm) on the left, right, and front sides.

To floor mount the cabinet:

1 Floor mount the cabinet as shown in Figure 56, Typical floor-mounted installation, on page 350.

Figure 56: Typical floor-mounted installation

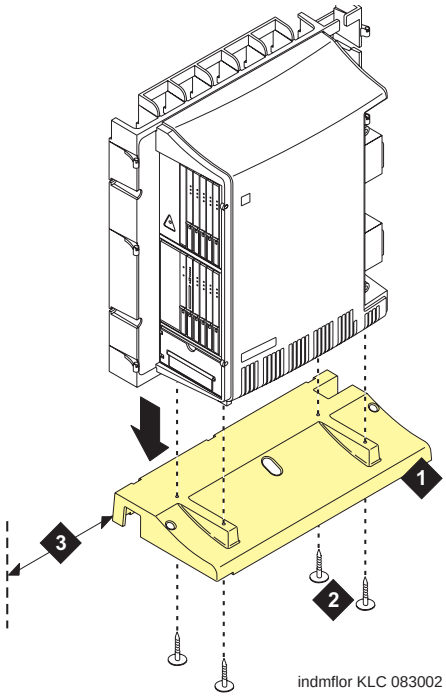


Figure notes

1 Left panel (floor-mounting pedestal)

2 #12 × 1-inch shoulder screws

3 12 inches (30.5 cm) minimum from nearest object (required to service the circuit packs)

2 Proceed to Check AC power and ground for CMC1 on page 357.

Wall mount the CMC1 cabinets

DANGER:
A fully loaded system with a single CMC1 cabinet weighs 58 lbs (26.3 kg). Use lifting precautions. The CMC1 unit weighs 29 lbs (13.1 kg) with the doors, power unit, and circuit packs removed.

Install plywood backing on wall

The install technician must provide the plywood and the hardware for mounting.

> **NOTE:**
> The following plywood dimensions account for the extra space needed to install the panels on each side of the cabinet. The cabinet is 24.5 inches (62.2 cm) wide, and each panel is 12 inches (30.5 cm) wide.

Single-cabinet installation

1. Install a ¾-inch (2-cm) thick sheet of 2- × 4-foot (0.6- × 1.2-m) plywood horizontally onto the wall. See Figure 57, Left panel used as mounting template, on page 352.
2. Ensure that the top of the plywood is at least 54 inches (1.37 m) from the floor.

Two vertically mounted cabinets

1. Install a ¾-inch (2-cm) thick sheet of 4- × 8-foot (1.2- × 2.4-m) plywood vertically onto the wall. See Figure 59, Typical vertical 3-cabinet installation, on page 354.

Two horizontally mounted cabinets

1. Install 2 ¾-inch (2-cm) thick sheets of 2- × 4-foot (0.6- × 1.2-m) plywood horizontally onto the wall. See Figure 60, Typical 3-cabinet installation, on page 355.
2. Position the 2nd sheet of plywood to the right of the 1st sheet.

Three vertically mounted cabinets

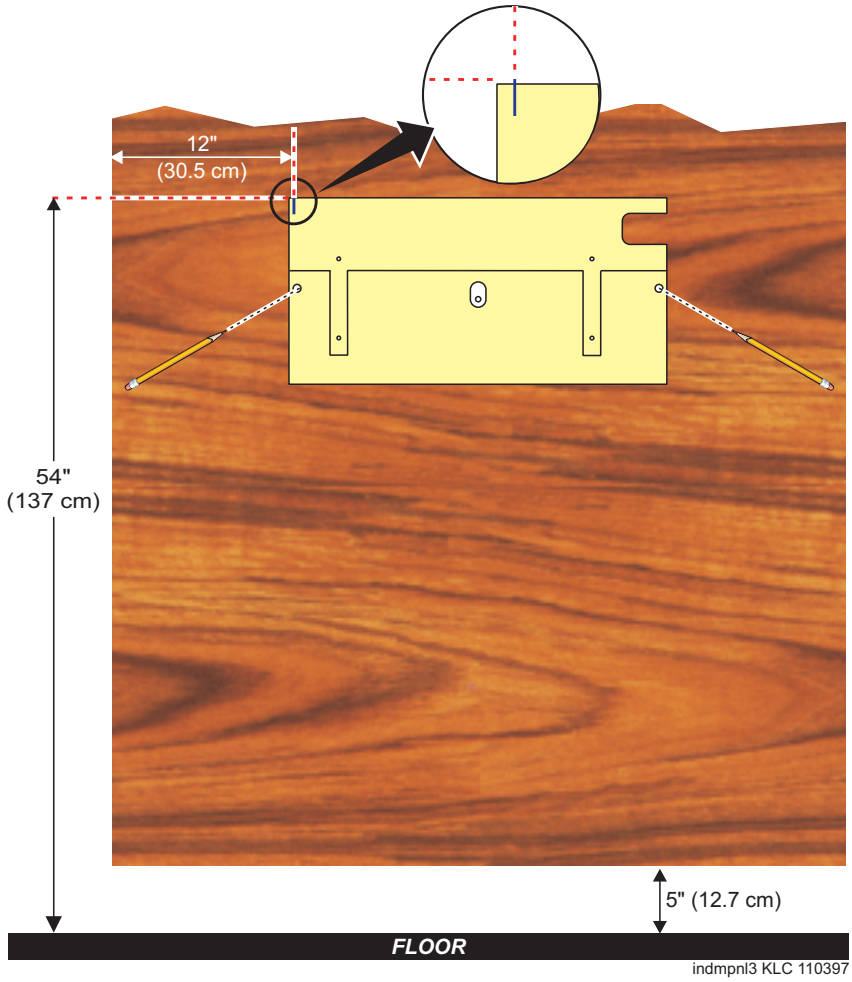
1. Install a ¾-inch (2-cm) thick sheet of 4- × 8-foot (1.2- × 2.4-m) plywood vertically onto the wall. See Figure 59, Typical vertical 3-cabinet installation, on page 354.

Three horizontally mounted cabinets

1. Install 2 ¾-inch (2-cm) thick sheets of 2- × 4-foot (0.6- × 1.2-m) plywood horizontally onto the wall. See Figure 60, Typical 3-cabinet installation, on page 355.
2. Position the 3rd sheet of plywood to the right of the 2nd sheet.

Install wall-mounted cabinet

Figure 57: Left panel used as mounting template



To mount a cabinet on a wall:

1. Place the template on the wall with the top surface level.
2. Mark 2 1/8-inch (0.3-cm) pilot holes to locate the mounting holes.
3. Remove the template from the wall.
4. Drill the 2 pilot holes.
5. Thread 2 #12 × 1-inch shoulder screws partially into the holes.
6. Set the cabinet onto the wall and align the slots with the shoulder screws. See Figure 58, Typical wall-mounted installation, on page 353. Slide the cabinet to the left to hold it in place. Tighten the screws securely.

Figure 58: Typical wall-mounted installation

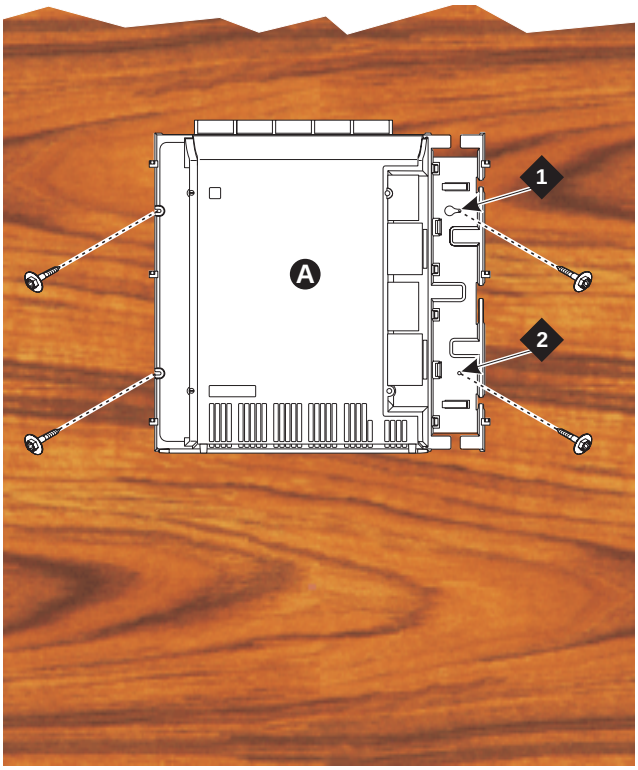


Figure notes

1	#12 × 1-inch shoulder screws	**2**	#12 × 1-inch safety screw

7 Drill 2 lower mounting holes using the cabinet as a template.

8 Thread the 2 lower screws and tighten.

WARNING:
Ensure that the right bottom safety screw is in place and tight.

Install three vertically mounted cabinets

Figure 59: Typical vertical 3-cabinet installation

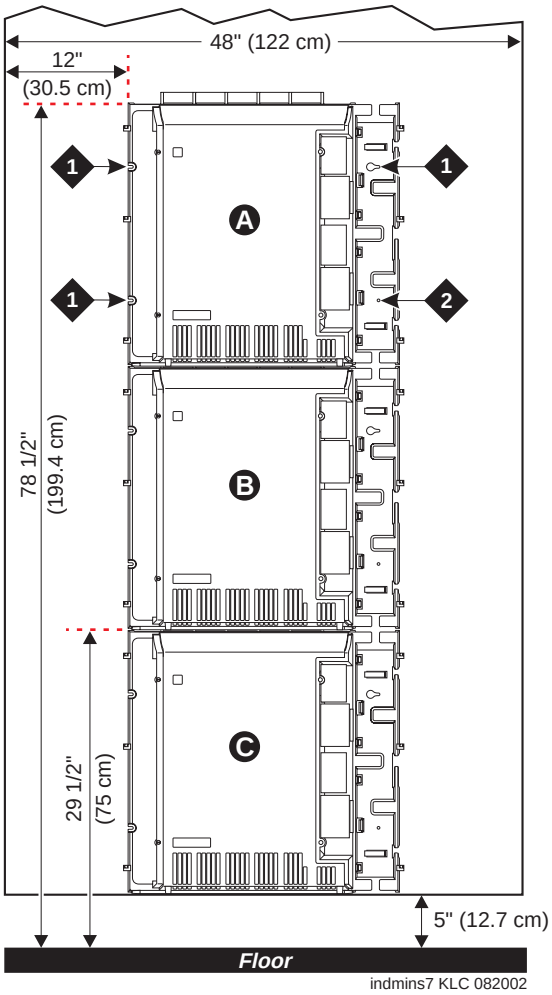


Figure notes

1	#12 × 1-inch shoulder screws	**2**	#12 × 1-inch safety screw

1 Securely tighten the shoulder screws and safety screws.

Install two cabinets vertically and one horizontally

Figure 60: Typical 3-cabinet installation

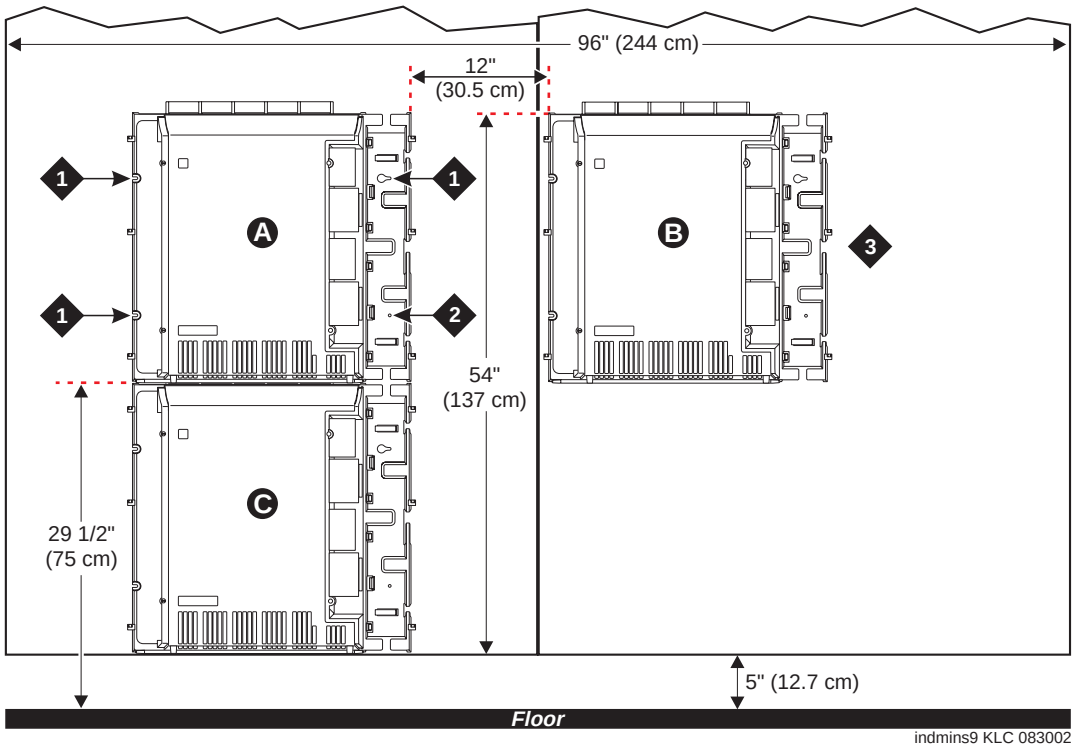


Figure notes

1	#12 × 1-inch shoulder screws	**3**	2nd sheet of plywood
2	#12 × 1-inch safety screw		

1 Securely tighten the shoulder screws and safety screws.

Install left and right panels – wall mount

Figure 61: Left and right panel installation

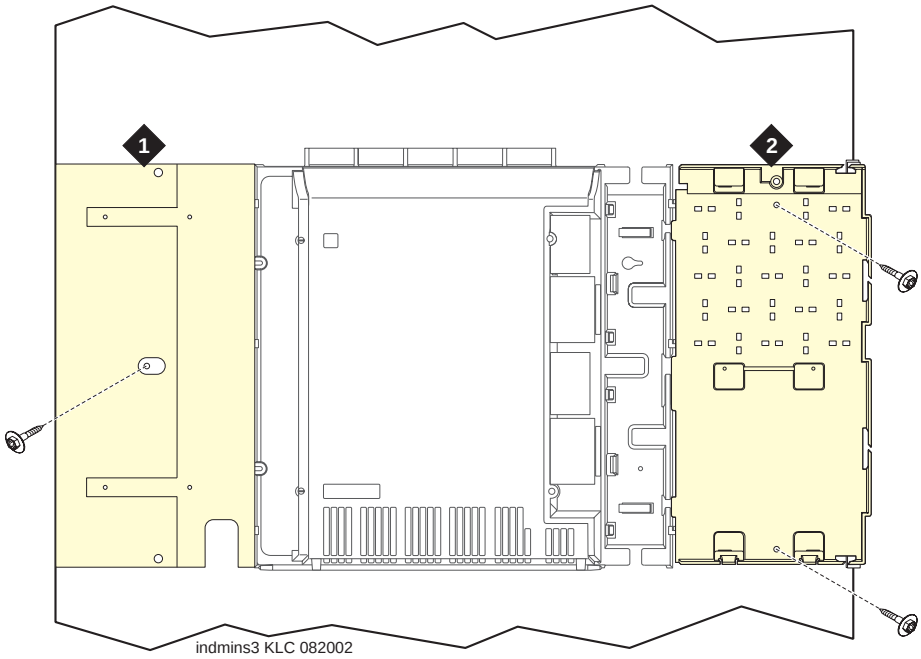


Figure notes

1	Left panel	**2**	Right panel

1. Align the cutouts in the panels with the cabinet's hinges.
2. Drill a 1/8-inch (3-mm) pilot hole into the wall and secure the panels with the #12 × 1-inch shoulder screws.
3. Proceed to Check AC power and ground for CMC1 on page 357.

Check AC power and ground for CMC1

WARNING:

The alternating current (AC) power circuit ***must be*** dedicated to the system. The circuit ***must not be*** shared with other equipment and ***must not be*** controlled by a wall switch. The AC receptacle ***must not be*** located under the CMC1's main distribution frame and ***must be*** easily accessible.

DANGER:

The latch only removes the cabinet's direct current (DC) power. Unseating the power supply removes AC power from the power supply, but not from the cabinet. To remove the cabinet's AC power, pull the AC power cord from the AC appliance connector behind the cabinet.

WARNING:

System grounding ***must comply*** with the general rules for grounding provided in Article 250 of the National Electrical Code (NEC), National Fire Protection Agency (NFPA) 70, or the applicable electric code in the country of installation.

WARNING:

AC mains wiring and testing ***must be performed*** by a qualified electrician and ***must conform*** to Article 250 of the NEC, NFPA 70, or the applicable electric code in the country of installation.

Check AC power

Each CMC1 uses an auto-ranging (85 to 264 VAC) power supply, 47 to 63 Hz, 330 Watts, 4.5 Amps (100 to120 VAC) or 2.3 Amps (200 to 240 VAC), at 500 VoltAmps (VA).

The AC power source can be 1 phase of 120 VAC with neutral (100 VAC for Japan) with 15-Amp circuit breaker, or 1 phase of 220 or 240 VAC (200 VAC for Japan) with 10-Amp circuit breaker. The AC cord uses a NEMA 5-15P plug or an IEC 320 plug.

Before powering up the system, check the AC power in the equipment room using a KS-20599 digital voltmeter (DVM) (or equivalent).

To check AC power:

1. Measure the AC voltage between the hot and neutral sides of the receptacle.
2. Depending on the AC power source, verify that the meter reads 90 to 132 VAC or 180 to 264 VAC. If not, have a qualified electrician correct the problem.
3. Measure the voltage between the neutral and ground sides of the receptacle.
4. Verify that the meter reads 0 VAC. If not, have a qualified electrician correct the problem.
5. When finished, set the AC main circuit breakers to ***OFF***.

Approved grounds

An approved ground is the closest acceptable medium for grounding the building entrance protector, entrance cable shield, or single-point ground of electronic telephony equipment. If more than one type of approved ground is available on the premises, the grounds must be bonded together as required in Section 250-81 of the National Electrical Code.

Grounded Building Steel – The metal frame of the building where it is effectively grounded by 1 of the following grounds: acceptable metallic water pipe, concrete-encased ground, or a ground ring.

Acceptable Water Pipe – A metal underground water pipe, at least ½ inch (1.3 cm) in diameter, in direct contact with the earth for at least 10 feet (3 m). The pipe must be electrically continuous (or made electrically continuous by bonding around insulated joints, plastic pipe, or plastic water meters) to the point where the protector ground wire connects. A metallic underground water pipe must be supplemented by the metal frame of the building, a concrete-encased ground, or a ground ring. If these grounds are not available, the water pipe ground can be supplemented by 1 of the following types of grounds:

- Other local metal underground systems or structures – Local underground structures such as tanks and piping systems
- Rod and pipe electrodes – A 5/8-inch (1.6-cm) solid rod or 3/4-inch (2-cm) conduit or pipe electrode driven to a minimum depth of 8 feet (2.4 m)
- Plate electrodes – Must have a minimum of 2 ft^2 (0.185 m^2) of metallic surface exposed to the exterior soil

Concrete Encased Ground – An electrode encased by at least 2 inches (5.1 cm) of concrete and located within and near the bottom of a concrete foundation or footing in direct contact with the earth. The electrode must be at least 20 feet (6.1 m) of 1 or more steel reinforcing bars or rods ½ inch (1.3 cm) in diameter, or at least 20 feet (6.1 m) of bare, solid copper, 4 AWG (26 mm^2) wire.

Ground Ring – A buried ground that encircles a building or structure at a depth of at least 2.5 feet (0.76 m) below the earth's surface. The ground ring must be at least 20 feet (6.1 m) of 2 AWG (35 mm^2), bare, copper wire.

Approved floor grounds

WARNING:
If the approved ground is inside a dedicated equipment room, then these connections must be made by a qualified electrician.

Floor grounds are those grounds on each floor of a high-rise building that are suitably connected to the riser closet's ground terminal and to the cabinet's single-point ground terminal. Approved floor grounds may include:

- Building steel
- The grounding conductor for the secondary side of the power transformer feeding the floor
- Metallic water pipes
- Power-feed metallic conduit supplying panel boards on the floor
- A grounding point specifically provided in the building for the purpose

Uninterruptible power supply

A recommended uninterruptible power supply (UPS) may be used for power holdover. The type of UPS depends on the holdover requirements. Total holdover capacity varies depending on the UPS. The UPS must provide surge protection for the CMC1 cabinet.

CAUTION:
The major-alarm contacts should ***only*** be connected to a UPS that can indicate its backup power status. For most non-Avaya UPSs, you should not use the major external device leads. Using these leads for anything else could cause an SPE download.

1. Connect the UPS to an electrical outlet capable of handling the power requirements of the cabinets:
   a. 100 VAC, 4.5 Amps
   b. 120 VAC, 3.8 Amps
   c. 200 VAC, 2.3 Amps
   d. 220 to 240 VAC, 2.0 Amps
2. Ensure that the cabinet is connected to an “unswitched” or “always-on” electrical outlet on the UPS.
3. For an Avaya-provided UPS, connect and administer the UPS. See Connect external alarms and auxiliary connections on page 113.

NOTE:
If an Avaya-provided UPS is wired as recommended, holdover time for each power outage is 1 minute before an automatic shutdown. The UPS may handle any subsequent power outages based on its total battery capacity.

Cabinet’s power switch

DANGER:
The latch acts as the DC power switch and only removes DC power from the cabinet, *not* AC power. To remove AC power, pull the AC power cord from the appliance inlet. See Figure 62, CMC1 power supply, on page 360.

Figure 62: CMC1 power supply

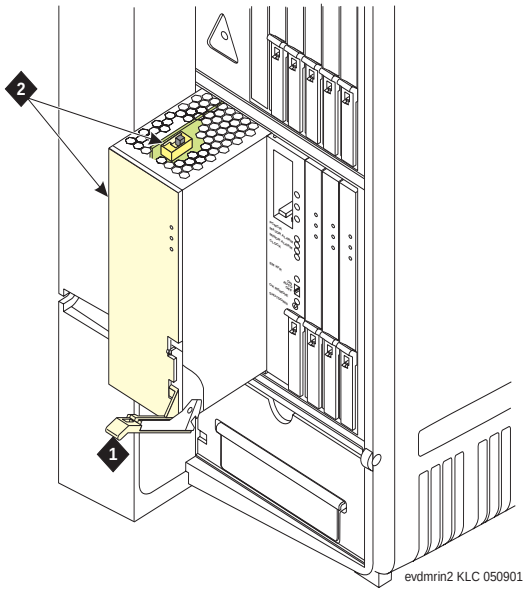


Figure notes

1	Latch	**2**	Ringing option switch and setting label

Connect cabinet's grounds and other grounds

Follow these additional grounding requirements:

- The approved ground wire must be green, 6 AWG (#40) (16 mm^2), copper, stranded wire. This is in addition to the ground wire in the AC power cord.
- Bond every approved ground at the single-point ground to form a single grounding electrode system.

Install the ground block and ground wire on cabinets

1 Mount the ground block as shown in Figure 63, Ground block installation to right CMC1 panel, on page 361.

Figure 63: Ground block installation to right CMC1 panel

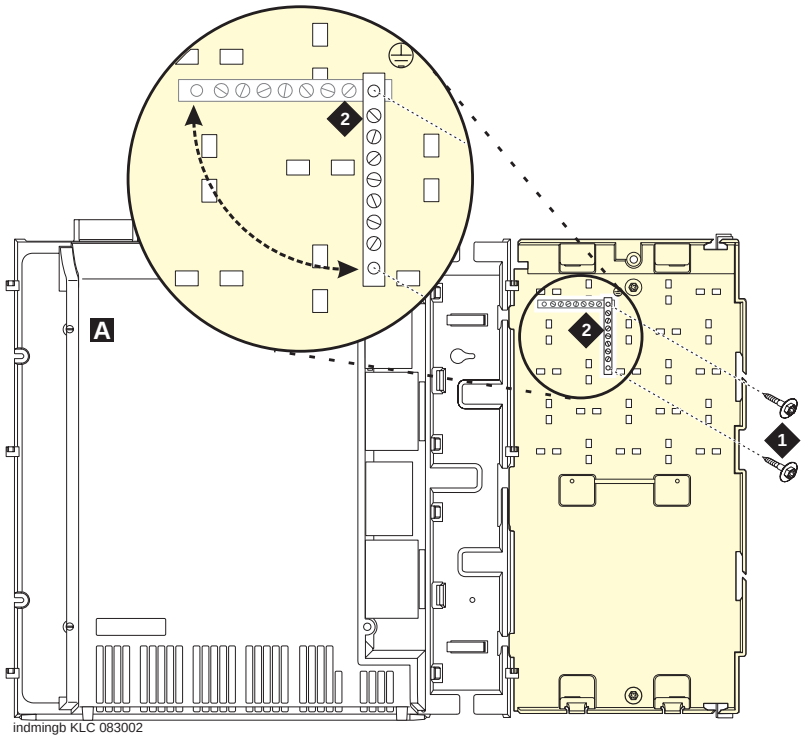
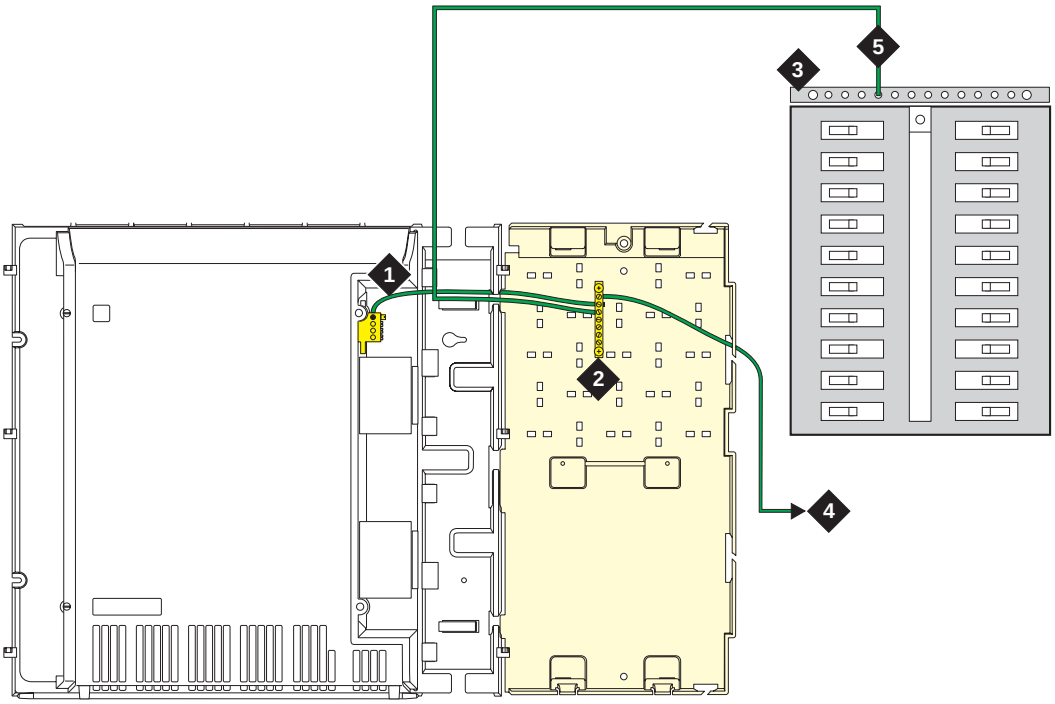


Figure notes

1	#12 × 1-inch shoulder screws	**2**	Single-point ground block

2 Connect the cable as shown in Figure 64, Typical single-cabinet CMC1 grounding, on page 362 for a single-cabinet CMC1 or Figure 65, Typical 2-cabinet CMC1 grounding, on page 363 for a 2-cabinet CMC1. Grounding a 3-cabinet configuration is similar to grounding the 2-cabinet configuration.

Figure 64: Typical single-cabinet CMC1 grounding



cadmgrd2 KLC 083002

Figure notes

1	6 AWG (#40) (16 mm^2) cabinet-ground wire	**4**	10 AWG (#25) (6 mm^2) wire to coupled bonding conductor (CBC)
2	Single-point ground block	**5**	6 AWG (#40) (16 mm^2) ground wire from single-point ground block to the AC load center's single-point ground
3	AC load center's single-point ground		

Figure 65: Typical 2-cabinet CMC1 grounding

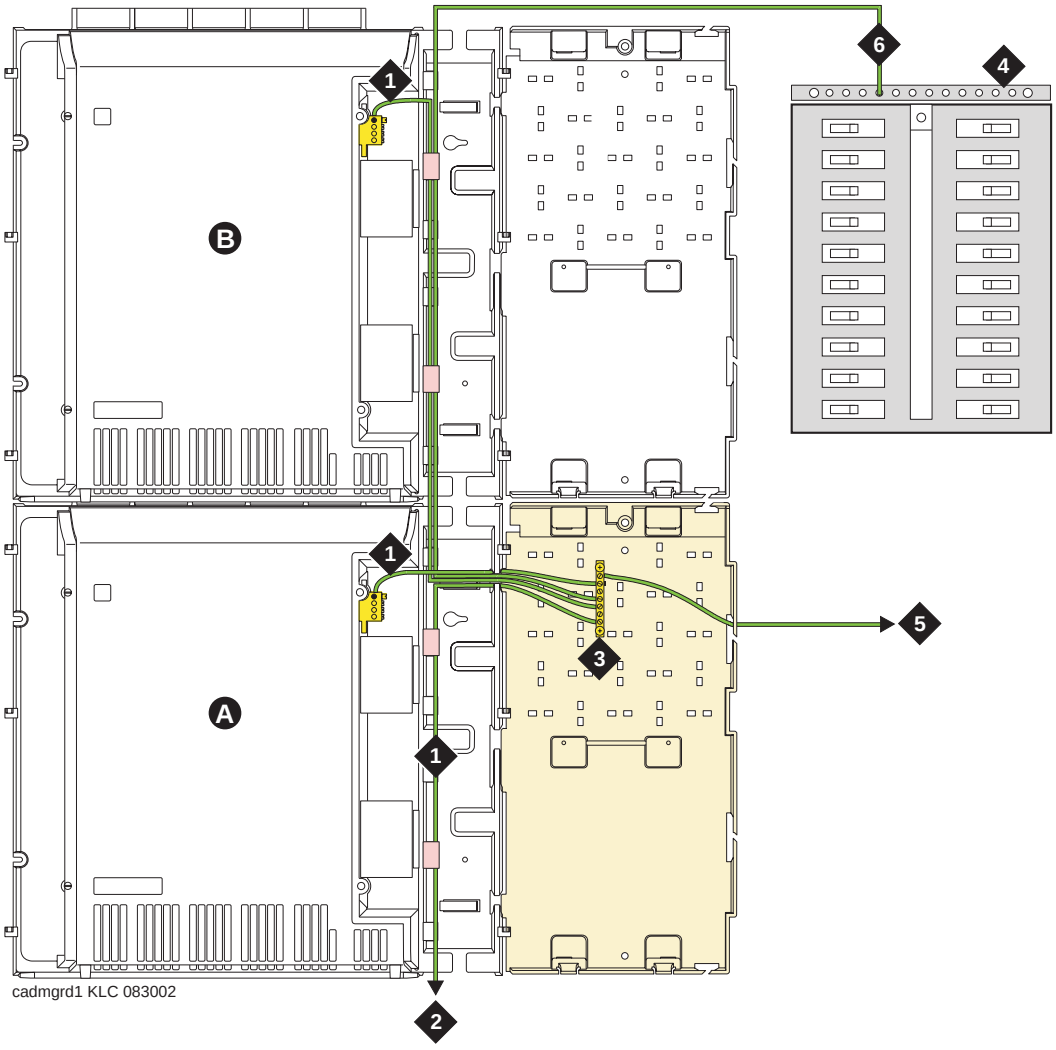


Figure notes

1 6 AWG (#40) (16 mm^2) cabinet-ground wire

2 6 AWG (#40) (16 mm^2) ground wire to next cabinet

3 Single-point ground block

4 AC load center's single-point ground

5 10 AWG (#25) (6 mm^2) wire to coupled bonding conductor (CBC)

6 6 AWG (#40) (16 mm^2) ground wire from single-point ground block to the AC load center's single-point ground

Install coupled bonding conductor

The coupled bonding conductor (CBC) provides mutual inductance coupling between the CBC and the telephone cables exposed to lightning. The conductor can be a 10 AWG (#25) (6 mm^2) wire tie wrapped to the exposed cables, a metal cable shield around the exposed cables, or 6 spare pairs from the exposed cable.

For a high-rise building, connect the CBC to an approved building ground on each floor. To provide the coupled bonding protection:

1. Connect one end of the conductor to a telephone cable building entrance protector ground that is connected to an approved ground.
2. Route the conductor next to the exposed telephone cables being protected until it reaches the cross-connect nearest to the telephone system.
3. Position the unexposed telephone cables at least 12 inches (30.5 cm) away from exposed telephone cables whenever possible.
4. Terminate the other end to the single-point ground block provided for the telephone system.

Connect and route the power cords

WARNING:
The AC power cord may connect to a properly rated power-distribution unit, individual AC power receptacles, or to a UPS.

See Figure 66, Routing a CMC1's AC power cord to power-distribution unit, on page 365 for CMC1 single-cabinet routing, Figure 67, Routing two CMC1s' AC power cords to power-distribution unit, on page 366 for CMC1 2-cabinet routing. Routing power cords for a 3-cabinet configuration is similar to routing the 2-cabinet configuration.

To connect and route the power cords:

1. Ensure the AC load center's circuit breakers are ***OFF***.
2. Connect the cabinet to an "unswitched" or "always-on" electrical outlet.

Figure 66: Routing a CMC1's AC power cord to power-distribution unit

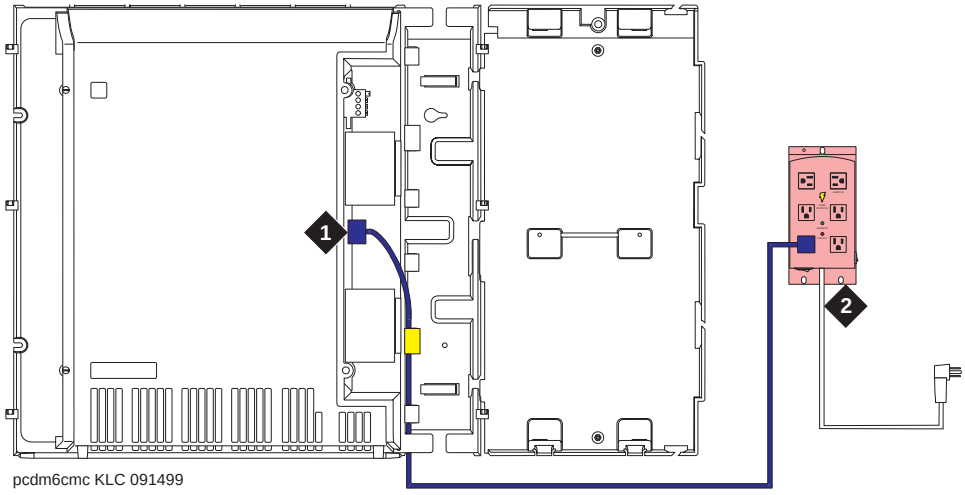


Figure notes

1	Cabinet's AC power cord	**2**	Surge-protected AC power-distribution unit (120-VAC systems) (optional)

Figure 67: Routing two CMC1s' AC power cords to power-distribution unit

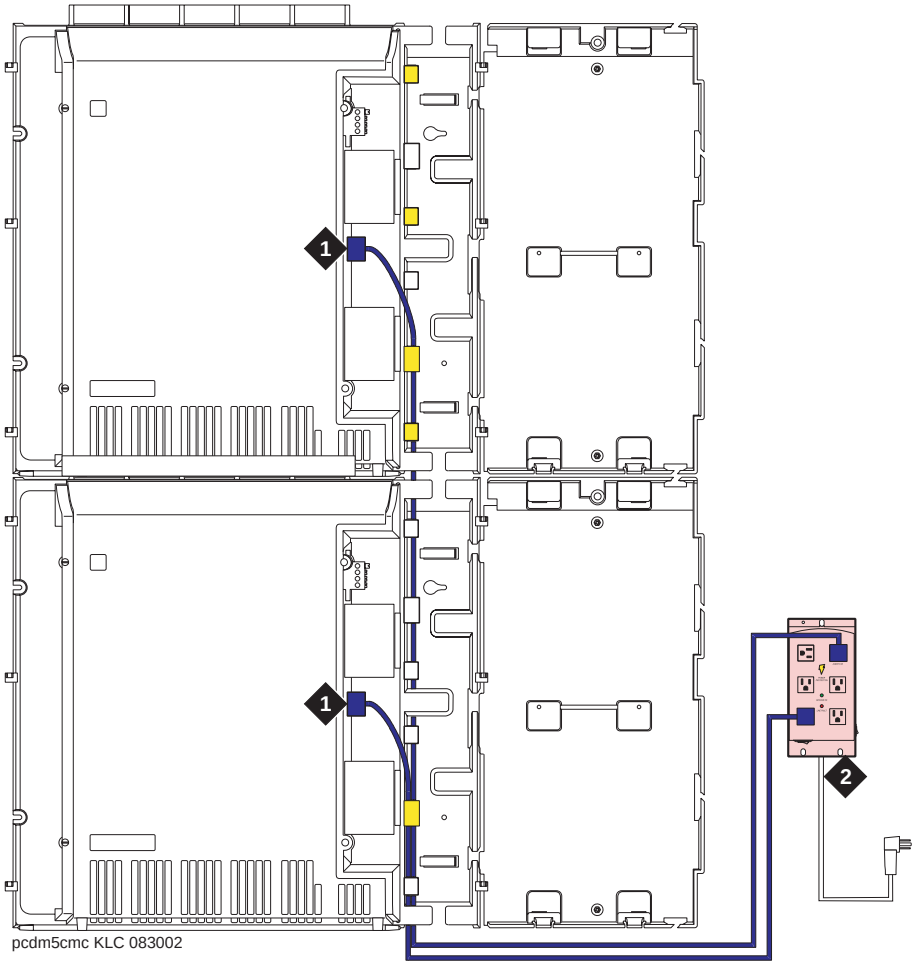


Figure notes

1	Cabinet's AC power cord	**2**	Surge-protected AC power-distribution unit (120-VAC systems) (optional)

Note: The power-cord routing for a 3-cabinet configuration follows the same pattern as the routing for the 2-cabinet configuration, shown here.

Cable a CMC1 system

Install Processor Interface cable and TDM-/LAN-bus terminators

Figure 68: CMC1 system's cable connections

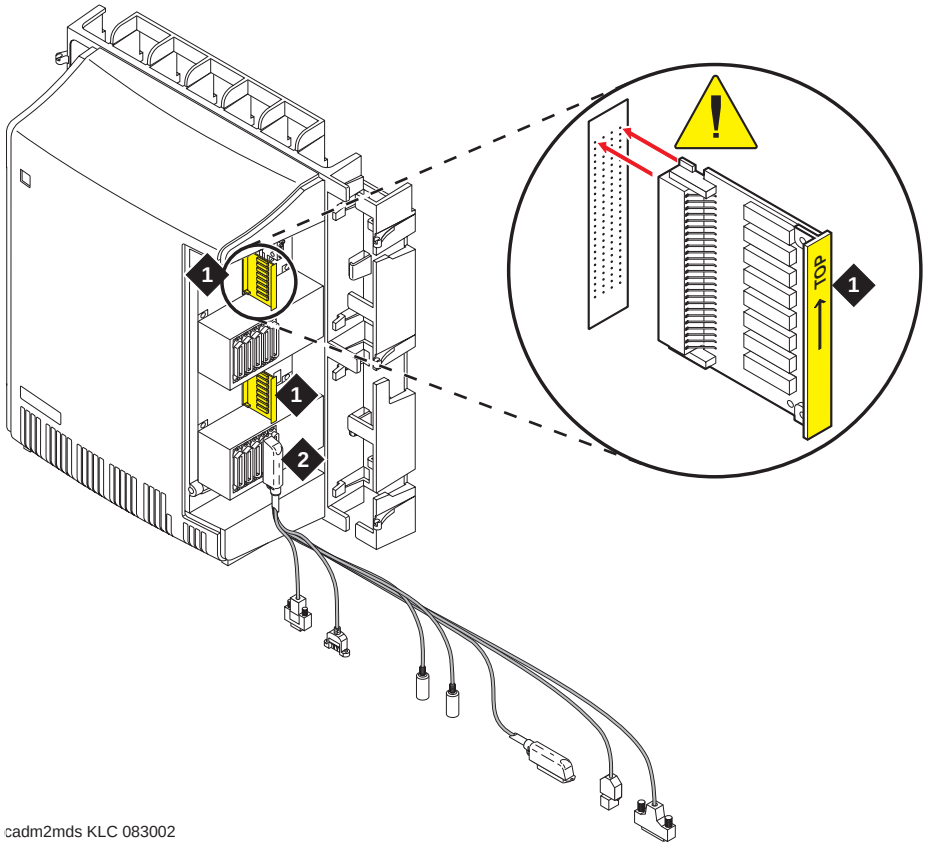


Figure notes

1	TDM-/LAN-bus terminators installed on the TDM-/LAN-bus pin fields	**2**	Processor Interface cable (slot 2)

1 Install the TDM-/LAN-bus terminators on the TDM-/LAN-bus pin fields.

2 Connect the Processor Interface cable to the slot 2 connector behind the cabinet. See Figure 68, CMC1 system's cable connections, on page 367.

Cable 3-cabinet CMC1 system

Vertically mounted system

1 Route the TDM-/LAN-bus cables through the cable trough. See Figure 69, System cable connections for three CMC1 cabinets vertically mounted, on page 368.

Figure 69: System cable connections for three CMC1 cabinets vertically mounted

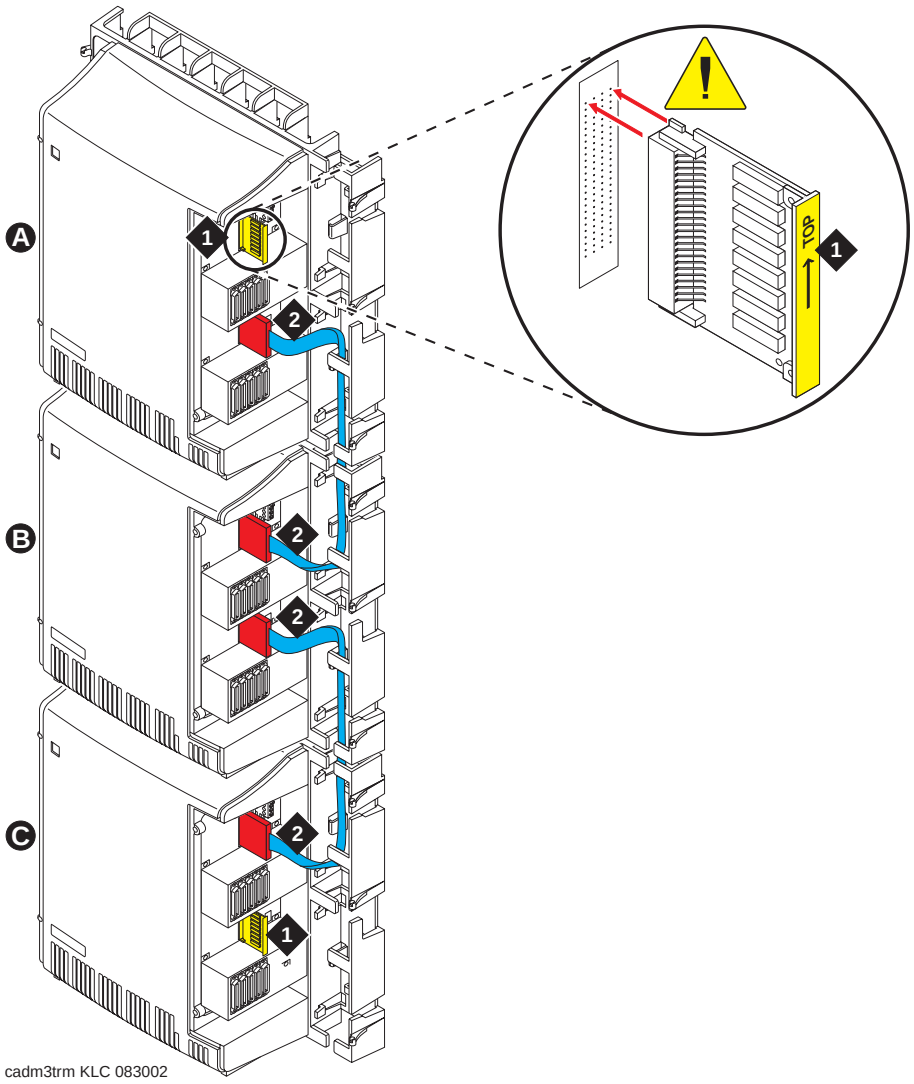


Figure notes

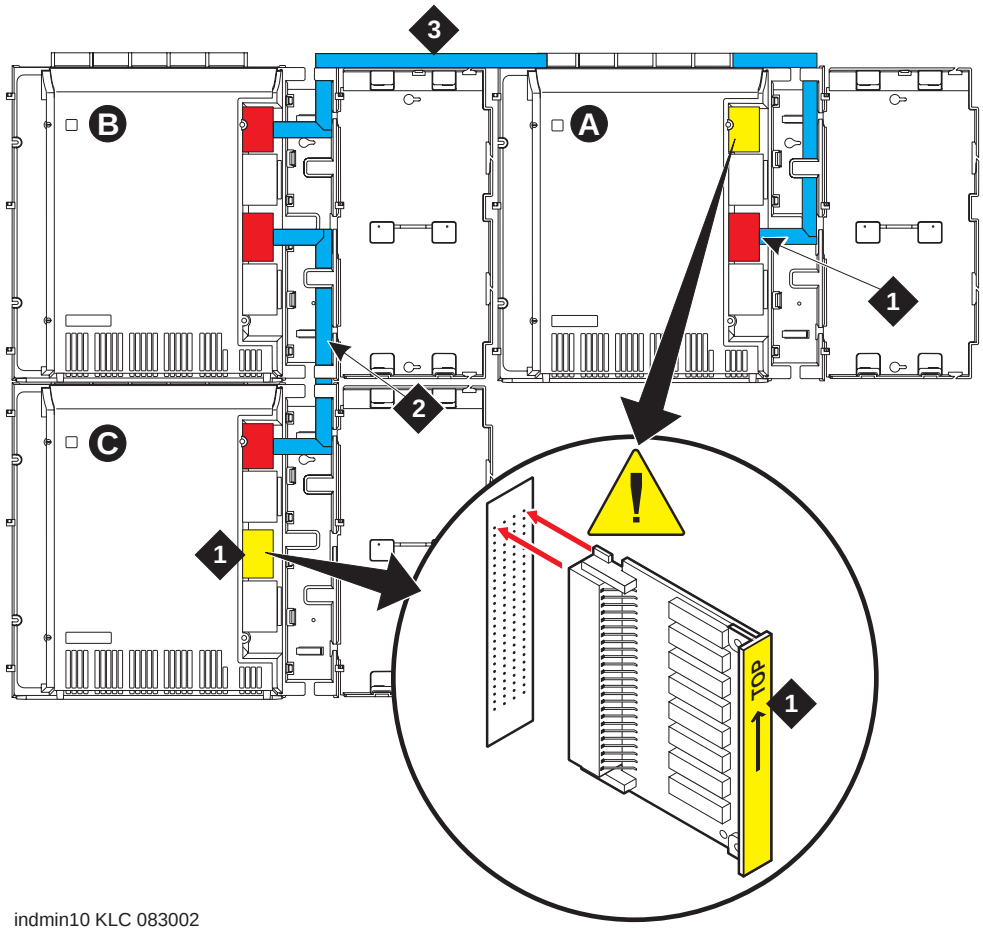
1 TDM-/LAN-bus terminators installed on the open TDM-/LAN-bus pin fields.

2 Vertical TDM-/LAN-bus cable (List 8)

Vertically and horizontally mounted system

1 Route the TDM-/LAN-bus cables through the cable trough. See Figure 70, System cable connections for three CMC1 cabinets vertically and horizontally mounted, on page 369.

Figure 70: System cable connections for three CMC1 cabinets vertically and horizontally mounted



indmin10 KLC 083002

Figure notes

1 TDM-/LAN-bus terminators installed on the open TDM-/LAN-bus pin fields.

2 Vertical TDM-/LAN-bus cable (List 8)

3 Horizontal TDM-/LAN-bus cable (List 9)

Install CMC1 main distribution frame (MDF) and external modem

Install the MDF on CMC1

WARNING:
The optional MDF is a special 110 cross-connect field that is smaller than the standard 110 cross-connect hardware. Do not install standard 110 hardware inside the right panel.

NOTE:
The depth of any equipment installed inside the right panel must not exceed 2.5 inches (6.3 cm), or the right cover panel will not fit over the right panel.

The optional MDF represents the trunk/auxiliary field.

- Mount the optional MDF to the right panel using the following procedure:

Bottom-mounted MDF with modem

1. Behind the MDF, cut the cable tie securing the top 5 cables to the MDF mounting frame.
2. Mount the MDF to the right panel. See Figure 71, Typical bottom-mounted MDF and modem cable routing, on page 371.
3. Secure all 10 cables to the bottom left bracket on the MDF with a cable tie.

Figure 71: Typical bottom-mounted MDF and modem cable routing

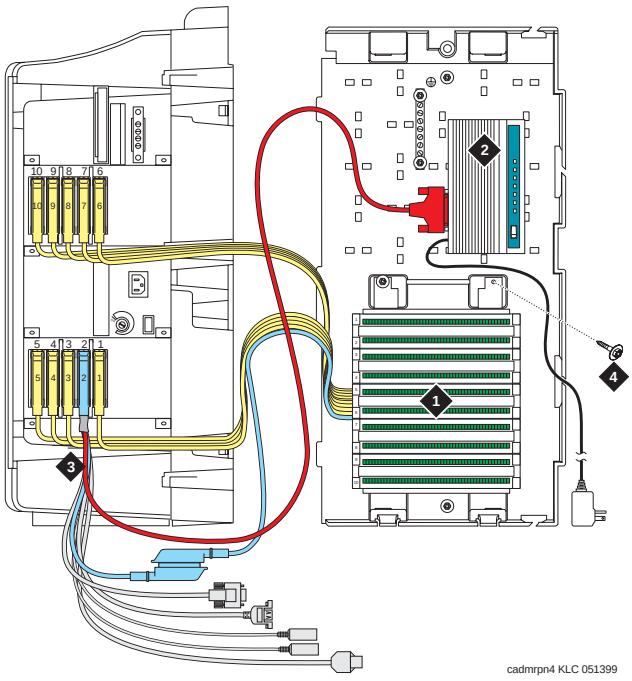


Figure notes

1	Main distribution frame (MDF)	**3**	Processor Interface cable (connect P2 to modem)
2	External modem	**4**	#12 × 1-inch shoulder screw

Note: Do not plug anything into slot 1 of Cabinet 1.

Install the external modem

The US Robotics external modem is the recommended external modem. CMC1 systems operate with this modem set to factory default settings.

NOTE:
You may use a locally obtained, type-approved external modem (33.6 kbps or higher and V.34 protocol). Contact your Avaya representative for more information.

WARNING:
If you use a modem other than the US Robotics modem, it must be configured in Windows.

1. Use the hardware provided with the modem. See Figure 71, Typical bottom-mounted MDF and modem cable routing, on page 371. If top-mounting MDFs, mount the external modem to the plywood in a location which allows the standard connection to the modem cable.
2. Route the modem cable (P2) from the Processor Interface cable through the cable trough and to the modem.

3 Connect the cable to the modem. See Appendix A, "Cable pinouts" for the pinout of the modem cable.

4 Plug the modem power cord into an electrical outlet and turn on the modem.

Modem's configuration and administration on page 262 describes information about modem setup, administration, settings, and testing.

Install equipment-room hardware for CMC1

See *DEFINITY Communications System Generic 1 and Generic 3 Main Distribution Field Design* (555-230-630) for more information.

Cross-connect the cabinet to the MDF

1 Cross-connect the port circuit packs to the CMC1 MDF. See Figure 73, Example MDF connections, on page 380.

Allowed circuit packs

Table 61, Allowed circuit packs and circuit modules, on page 372 lists the circuit packs that can be used with CMC1. (Table 62, Disallowed circuit packs and circuit modules, on page 375 lists the circuit packs that cannot be used with CMC1).

Table 61: Allowed circuit packs and circuit modules ***1 of 3***

Apparatus code	Name	Allowed?
650A	AC power unit	Yes
NAA1	Fiber-Optic Cable Adapter circuit pack	Yes
TN417	Auxiliary Trunk	Yes
TN429/B/C/D	Analog Direct Inward/Outward Dialing (DIOD) Central Office Trunk	Yes
TN429C	Analog Central Office Trunk	Yes
TN429D	Analog DIOD Trunk – Analog Loop Start	Yes
TN433	Speech Synthesizer	Yes
TN436B	Direct Inward Dialing Trunk	Yes
TN437B	Tie Trunk Australia (future availability)	Yes
TN438B	Central Office Trunk	Yes
TN439	Tie Trunk	Yes

1 of 3

Table 61: Allowed circuit packs and circuit modules ***2 of 3***

Apparatus code	Name	Allowed?
TN447	Central Office Trunk	Yes
TN457	Speech Synthesizer	Yes
TN459B	Direct Inward Dialing Trunk	Yes
TN464GP	DS1 Interface – T1, 24 Channel - E1, 32 Channel	Yes
TN465B/C	Central Office Trunk	Yes
TN467	Analog Line	Yes
TN468B	Analog Line	Yes
TN479	Analog Line	Yes
TN553	Packet Data Line	Yes
TN556C/D	Integrated Services Digital Network -Basic Rate Interface 4-Wire S/T-NT Interface (ISDN-BRI)	Yes
TN722B	DS1 Tie Trunk	Yes
TN725B	Speech Synthesizer	Yes
TN726B	Data Line	Yes
TN735	Multibutton Electronic Telephone (MET) Line	Yes
TN742	Analog Line	Yes
TN744E	Call Classifier – Detector	Yes
TN746B	Analog Line	Yes
TN747/B	Central Office Trunk	Yes
TN750C	Announcement	Yes
TN753/B	Direct Inward Dialing Trunk	Yes
TN754/B/C	Digital Line 4-Wire DCP	Yes
TN758	Pooled Modem	Yes
TN760B/C/D/E	Tie Trunk	Yes
TN762/B	Hybrid Line	Yes
TN763B/C/D	Auxiliary Trunk	Yes
TN767B/C/D/E	DS1 Interface – T1, 24 Channel	Yes
TN769	Analog Line	Yes
TN771/D	Maintenance/Test	Yes

2 of 3

Table 61: Allowed circuit packs and circuit modules ***3 of 3***

Apparatus code	Name	Allowed?
TN789	Radio Controller	Yes
TN791	Analog Line	Yes
TN793	Analog Line, 24-Port, 2-Wire	Yes
TN2314	Processor	Yes
TN799DP	Control LAN (C-LAN)	Yes
TN802/B	Internet Protocol (IP) Trunk	Yes
TN2135	Analog Line	Yes
TN2136	Digital Line 2-Wire DCP	Yes
TN2138	Central Office Trunk	Yes
TN2139	Direct Inward Dialing Trunk	Yes
TN2140B	Tie Trunk – Hungary, Italy	Yes
TN2144	Analog Line	Yes
TN2146	Direct Inward Dialing Trunk	Yes
TN2147C	Central Office Trunk	Yes
TN2149	Analog Line	Yes
TN2180	Analog Line	Yes
TN2181	Digital Line 2-Wire DCP	Yes
TN2183	Analog Line	Yes
TN2184	DIOD Trunk	Yes
TN2185/B	ISDN-BRI 4-Wire S/T-TE Interface (Trunk Side)	Yes
TN2199	Central Office Trunk	Yes
TN2207	DS1 Interface – (T1) 24 Channel and (E1) 32 Channel	Yes
TN2224/B	Digital Line, 24-Port, 2-Wire DCP	Yes
TN2242	TTC Japanese 2-Mbit Trunk	Yes
TN2302	IP Media Processor	Yes
TN2305	Asynchronous Transfer Mode (ATM) Trunk	Yes
TN2464	DS1 Interface – T1, 24 Channel - E1, 32 Channel	Yes
TN2793/B	Analog Line 24-Port	Yes

3 of 3

Disallowed circuit packs

Table 62, Disallowed circuit packs and circuit modules, on page 375 lists the circuit packs that cannot be used with CMC1.

Table 62: Disallowed circuit packs and circuit modules ***1 of 2***

Apparatus code	Name	Allowed?
982LS	Current Limiter	No
CFY1B	Current Limiter	No
CPP1	Memory Expansion	No
ED-1E546 (TN566) (TN567)	INTUITY AUDIX R3 System	No
ED-1E546 (TN2208) (TN2170)	CallVisor Adjunct-Switch Application Interface (ASAI) over the DEFINITY LAN Gateway R1	No
J58890M-1 (TN801)	CallVisor ASAI/Call Visor PC/LAN over the DEFINITY LAN Gateway Release 2.0	No
TN419B	Tone-Clock	No
TN420B/C	Tone Detector	No
TN568	INTUITY AUDIX Slim	No
TN570B/C	Expansion Interface	No
TN572	Switch Node Clock	No
TN573B	Switch Node Interface	No
TN574	DS1 Converter – T1, 24 Channel	No
TN577	Packet Gateway	No
TN748B/C/D	Tone Detector	No
TN750B	Announcement	No
TN755/B	Neon power unit	No
TN756	Tone Detector/Generator	No
TN765	Processor Interface	No
TN768	Tone-Clock	No
TN772	Duplication Interface	No
TN775/B/C	Maintenance	No

1 of 2

Table 62: Disallowed circuit packs and circuit modules ***2 of 2***

Apparatus code	Name	Allowed?
TN776	Expansion Interface	No
TN777B	Network Control	No
TN778	Packet Control	No
TN780	Tone-Clock	No
TN787F/G/H/J/K	Multimedia Interface	No
TN788B	Multimedia Voice Conditioner	No
TN790B	Processor	No
TN792	Duplication Interface	No
TN794	Network Control/Packet Interface (NetPkt)	No
TN798B	Processor	No
TN801	LAN Gateway Interface	No
TN1648/B	System Access/Maintenance	No
TN1650B	Memory	No
TN1654	DS1 Converter – T1, 24 Channel/E1, 32 Channel	No
TN1655	Packet Interface	No
TN1656	Tape Drive	No
TN1657	Disk Drive	No
TN2182/B	Tone-Clock – Tone Detector and Call Classifier	No
TN2198	ISDN-BRI 2-Wire U Interface	No
TN2202	Ring Generator	No
TN2210	Tone Generator	No
TN2214/B	Digital Line, 24-Port, 2-Wire DCP – Category B only	No
TN2215	Analog Line, 16-Port 2-Wire – Category B only	No
TN2238	ATM Trunk Interface (multimode)	No
TN2301	Survivable Remote Logic Switch	No
TN2306	ATM Interface (single-mode)	No
TN2308	Direct Inward Dialing Trunk	No

2 of 2

Circuit pack installation

WARNING:

When handling circuit packs or any components of a CMC1, always wear an authorized wrist ground strap. Connect the strap to the ground connector provided on the system's cabinet.

Circuit-pack slot loading

Every circuit-pack slot in the CMC1 is a "universal slot." Any slot can contain any type of port circuit pack, with the following exceptions for Cabinet A.

1. Install the TN2314 Processor circuit pack in slot 2. See Figure 72, CMC1 cabinet and slot numbering, on page 378.
2. Install the required TN744E Call Classifier/Tone Detector circuit pack in slot 3.
3. Load a port circuit pack in every other slot. See Table 63, Circuit-pack installation order (loading), on page 378 for the recommended circuit-pack layout.

Figure 72: CMC1 cabinet and slot numbering

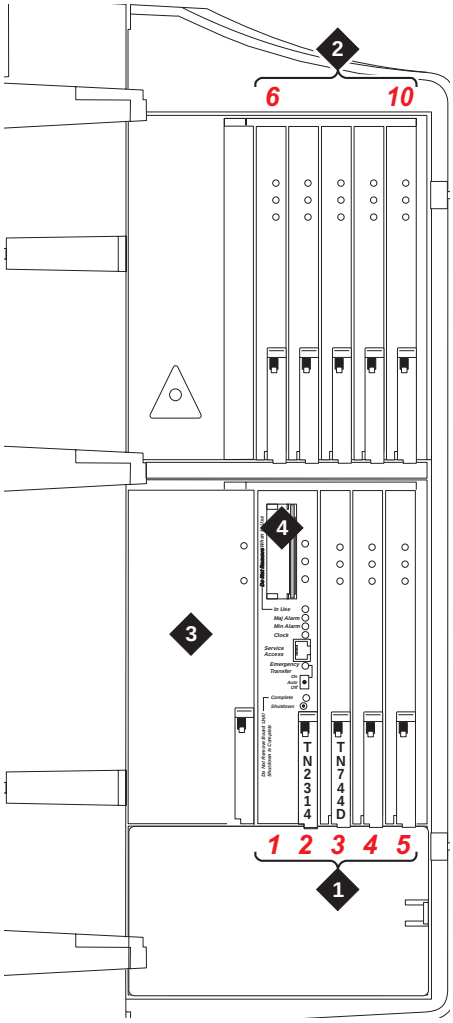


Figure notes

1	Slots 1 – 5	**3**	650A power unit
2	Slots 6 – 10	**4**	For flash disk (PCMCIA)

Table 63: Circuit-pack installation order (loading) ***1 of 2***

Function	Apparatus code	Load CMC1 from	Notes
Processor	TN2314	Slot 1 and 2	
Call Classifier/Tone Detector	TN744E	Slot 3	
Announcement	TN750C	Any slot	
Speech Synthesizer	TN725B	Any slot	
Control C-LAN	TN799DP	Lower right	

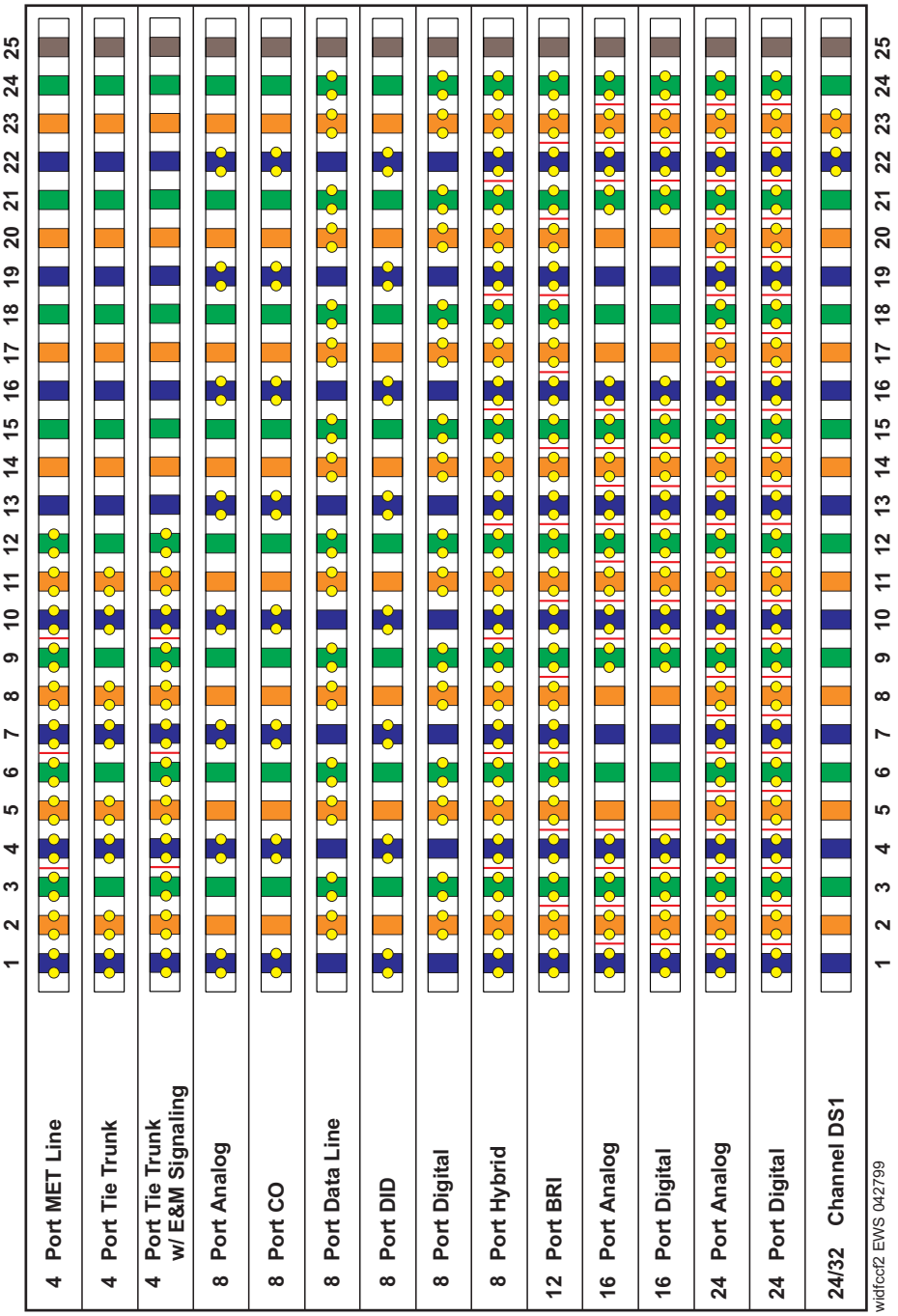
1 of 2

Table 63: Circuit-pack installation order (loading) ***2 of 2***

Function	Apparatus code	Load CMC1 from	Notes
Media Processor	TN2302	Lower right	
DS1/E1, ISDN-PRI	TN464GP, TN767E, TN2242, TN2464	Lower right	Maximum of 7 – Total number of ISDN-PRI **and** ISDN-BRI circuit packs must not exceed 7.
ISDN-BRI Trunk	TN2185	Lower right	Maximum of 4
CO Trunk	TN747B, TN465C, TN2199, TN2147C, TN2138, TN438B	Lower right	
DID Trunk	TN753, TN2139, TN2146, TN436B, TN459B	Lower right	
Tie Trunk	TN760E, TN458, TN497, TN2140B	Lower right	
Auxiliary Trunk	TN417	Lower right	
Modem Pool	TN758	Lower right	
Data Line	TN726	Upper left	
Digital Line	TN754C, TN2181, TN2224/B	Upper left	
Analog Line	TN746B, TN2135, TN467, TN2144, TN2149, TN2180, TN2183, TN2215, TN468B, TN791, TN793, TN2793, TN2214	Upper left	
Hybrid Line	TN762B	Upper left	
MET Line	TN735	Upper left	
Radio Controller	TN789	Upper left	
ISDN-BRI 4-Wire S/T-NT Line (A-Law)	TN556C/D	Upper left	

2 of 2

Figure 73: Example MDF connections



Off-premises circuit protection

Protection from hazardous voltages and currents is required for every off-premises (out-of-building) trunk, line, or terminal installation. Both over-voltage protection (lightning, power induction, and so forth) and sneak-current protection are required. Sneak-current protectors must be either UL-listed or CSA-certified, or must comply with local safety standards.

Sneak-current protectors must have a maximum rating of 350 mA and a minimum voltage rating of 600V, or as required by local regulations. The following devices protect the system from over-voltages:

- Analog trunks use the 507B sneak protector or equivalent. Over-voltage protection is normally provided by the local telephone company.
- Analog voice terminals use one of the following types of combined over-voltage and sneak-current protection, or equivalent:
  - — Carbon block with heat coil for UL code 4B1C
  - — Gas tube with heat coil for UL code 4B1E-W
  - — Solid state with heat coil for UL code 4C1S
- DCP and ISDN-BRI terminals use the solid state 4C3S-75 with heat coil protector, or equivalent.
- DS1/T1 circuits require isolation from exposed facilities. This isolation may be provided by a channel-service unit (CSU) (T1), or other equipment that provides equivalent protection.

Install sneak fuse panels

Sneak-current protection is required between the incoming RJ21X or RJ2GX network interface and the system for both trunk and off-premises circuit packs. The model 507B sneak-current fuse panel, or equivalent, is recommended for sneak-current protection. See Figure 74, Model 507B sneak fuse panel, on page 381.

Figure 74: Model 507B sneak fuse panel

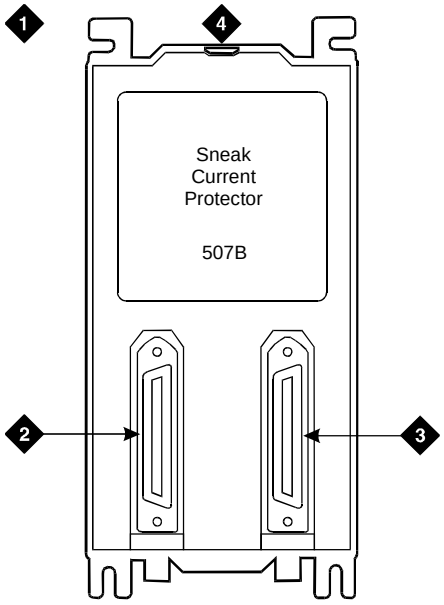


Figure notes

1	507B sneak-current protector (comcode 107435091)	**3**	25-pair female connector (out) (comcode 846300994)
2	25-pair male connector (in) (comcode 846300994)	**4**	220029 fuses (inside panel) – Use a small screwdriver to pry top cover off.

Each column of sneak fuse panels requires approximately 8 inches (20 cm) of horizontal wall space. Connector cables connect the network interface to the sneak fuse panel. Also, use 157B connecting blocks equipped with SCP-110 protectors for sneak-current protection.

NOTE:
Sneak-current protectors with a rating of 350 mA at 600 V must be UL-listed for United States installations or CSA-certified for Canadian installations. The panel contains 2 25-pair connectors, fuse removal tool, and fifty 220029 sneak fuses (and 2 spares). Use the SCP-110 protectors with 110-type hardware and on the 507B sneak fuse panel. The SCP-110 protectors can be ordered separately and installed on the 157B connecting block. Fifty protectors are required per block.

1 Install the 507B near the network interface or MDF with locally-obtained #12 × ¾-inch screws (or equivalent).

Table 64, Sneak fuse connector pinout, on page 382 is a pinout of the cable wiring and associated fuse numbers.

Table 64: Sneak fuse connector pinout ***1 of 2***

Connector pin numbers	Pair/fuse number
26/1	1
27/2	2
28/3	3
29/4	4
30/5	5
31/6	6
32/7	7
33/8	8
34/9	9
35/10	10
36/11	11
37/12	12
38/13	13
39/14	14
40/15	15
41/16	16
42/17	17
	1 of 2

Table 64: Sneak fuse connector pinout ***2 of 2***

Connector pin numbers	Pair/fuse number
43/18	18
44/19	19
45/20	20
46/21	21
47/22	22
48/23	23
49/34	24
50/25	25
	2 of 2

Label the main distribution frame

Figure 75, Label graphic symbols and nomenclature, on page 384 shows the graphic symbols used on the supplied labels for the system, cross-connections, information outlets, and cables.

1. Write the floor and building identification on each label as required.
2. Insert the labels into the plastic holders.
3. Snap the holders into the appropriate locations on the MDF.

Figure 75: Label graphic symbols and nomenclature

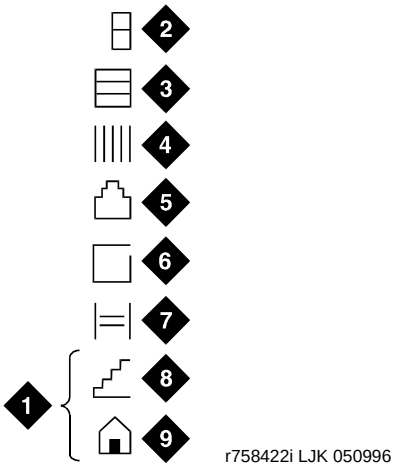


Figure notes

1	Floor and building identification	**6**	Site/satellite closet
2	Cabinet	**7**	Tie circuit
3	Carrier	**8**	Floor
4	Slot	**9**	Building
5	Information outlet		

4 Label the cables as required using the supplied labels. Label code number 220A (comcode 103970000) contains every required label.

Set ringing option for CMC1

Figure 76: Selection of ringing option

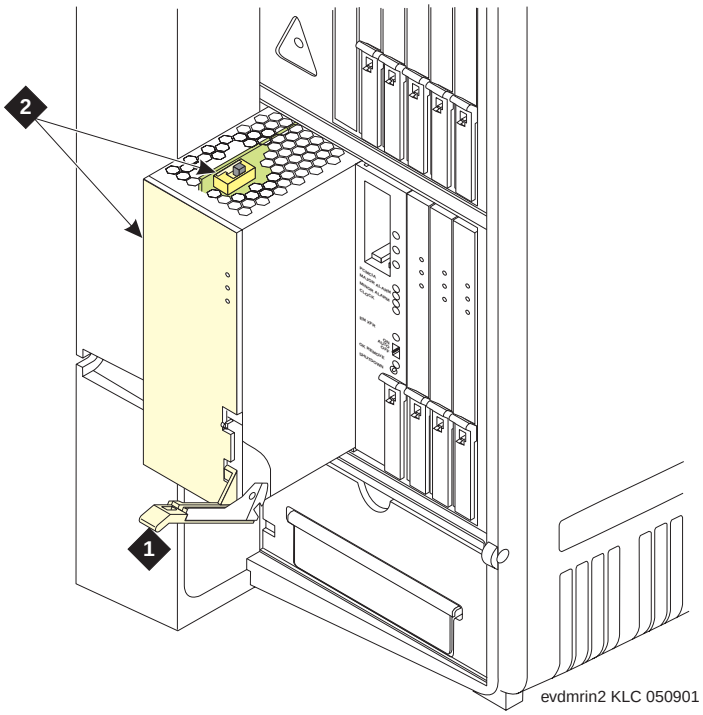


Figure notes

1 Attachment lever

2 Ringing option switch and setting label

Note: Look at the label on the side of the power supply to see how to set the switch.

Figure 77: TN2314 circuit pack's faceplate

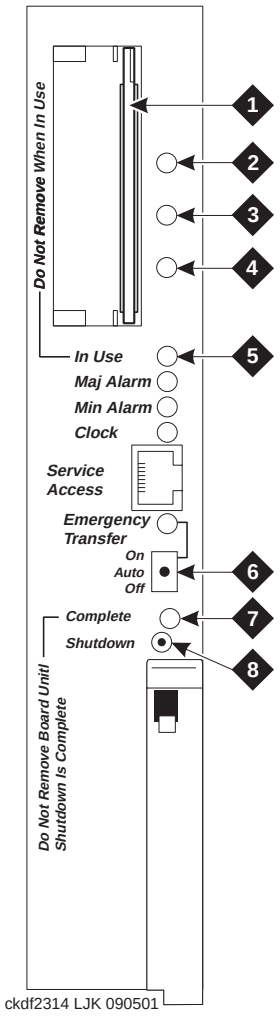


Figure notes

1	PCMCIA slots	**5**	PCMCIA in-use LED
2	Red LED	**6**	Emergency Transfer switch
3	Green LED	**7**	Shutdown-complete LED – Safe to pull board when green LED is on
4	Amber LED	**8**	Shut-down switch – Gracefully shuts down system

K Identify a hard disk for PCN1413b

This appendix provides the steps to identify the correct hard disks to be replaced under PCN1413b.

NOTE:
Follow either Steps 1–3 of this procedure for an S8100's installation or the entire procedure (except Step 3) for routine maintenance operations.

If an S8100's hard drive appears unreliable, identify whether the hard drive should be replaced.

1. Peel away the label on the hard drive to find its model number.
2. If the the hard drive's model number matches the one shown in the following figure (IC25N020ATCS04-0):

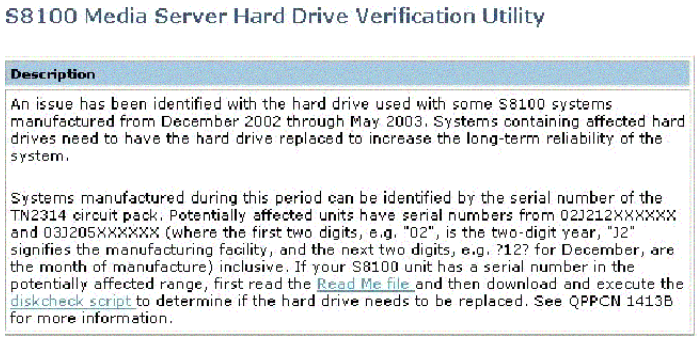
   This model has been identified as unreliable (as an S8100 drive) and should be replaced under PCN1413b.

3. If you are ***installing*** a new S8100, then either:
   - — Contact the TSO for a case number authorizing the DOA hard drive's replacement.
   - — For an Avaya installation, inform the project manager that the hard drive needs to be replaced.

   and (once the new drive is acquired) continue with Replace an S8100's hard drive on page 20. If ***not***, continue with Step 4.
4. For a repair or a preventative maintenance activity, then access the "http://support.avaya.com" website to download the "diskcheck" file.
5. Once at the Avaya Support website, access the diskcheck file's specific web page by:
   - **a** Clicking the Software and Firmware Downloads link.
   - **b** Under the heading "Enterprise Class IP Solutions," clicking the S8100 Media Server link.
   - **c** Clicking the Software Downloads link.
   - **d** Clicking the S8100 Media Server Hard-Drive Verification utility.

The following figure shows a portion of this web page:

NOTE:
For this specific activity, ***neither*** the hard drive's TN number ***nor*** serial number are relevant. The following description is only intended as a guide.



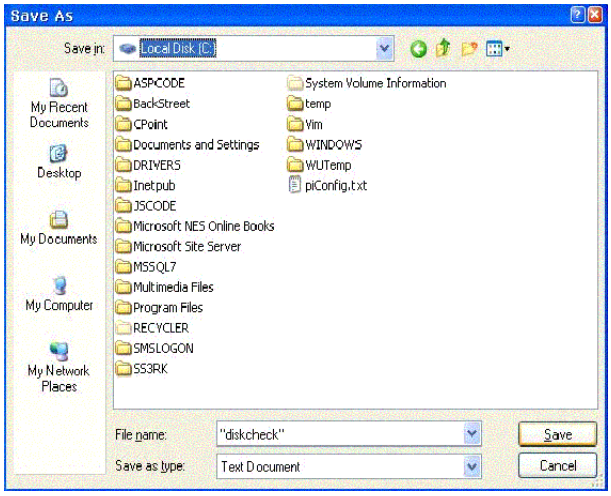
6 Download the diskcheck file to your laptop:

a Right-click the highlighted item "diskcheck script".

b From the help menu, click "Save Target As…".

c From the Save As dialog, save the binary "diskcheck" file to a convenient folder and your chosen name on your local C:\ drive, as shown in the following figure.

NOTE:
Be sure to enter quotation marks around the file's chosen name to maintain the file's binary integrity.



d Click the Save button.

7 Connect to the customer's S8100 system.

For detailed information, refer to Connectivity and access to an S8100 system on page 139.

8 Open a CMD (Command) window on your laptop:

   a Click Start → Run, and then type **cmd** in the Run dialog.

   b Click the OK button.

9 Using the S8100 system's IP address, Telnet to and log into the system.

   NOTE:
   Depending on your specific login credentials, the system returns either the LAC or BASH prompt.

10 Access the bash shell (if necessary), and use it for the rest of this procedure.

11 At the BASH prompt, enter **ftpserv** to start the FTP service.

12 Open another CMD (Command) window on your laptop. (For details, refer to Step 8.)

13 Enter **ftp -A [IP Address]** to open an FTP session with the S8100.

14 At the ftp> prompt, transfer the diskcheck file to the S8100:

   a Enter **bin** to set up a binary transfer.

   b Type **mput diskcheck**, and then type "**y**" to execute the transfer.

15 When the transfer finishes, enter **bye** to exit the FTP service.

16 Access the S8100's diskcheck utility:

   a At your laptop, reopen (toggle back to) the other CMD window.

   a Enter **cd //d/lucentpub/ftproot**.

   b Enter **pwd** to verify the S8100's current directory.

17 Enter **./diskcheck** to verify whether the hard drive needs to be replaced. If so, the utility returns a message similar to:

```
REPLACE      2 IBM-DJSA-220
```

   Once the new drive is acquired, continue with Replace an S8100's hard drive on page 20.

Glossary

A

AAR
See Automatic Alternate Routing (AAR) on page 391.

AC
1. Alternating current.
2. See analog.

Access Security Gateway (ASG)
A feature built into the Lucent Access Control (LAC) module that authenticates and protects logins to the LAC.

administer
To access and change parameters associated with the services or features of a system.

analog
The representation of information by continuously variable physical quantities such as amplitude, frequency, and phase. See also, digital on page 393.

analog data
Data that is transmitted over a digital facility in analog (PCM) form. The data must pass through a modem either at both ends or at a modem pool at the distant end.

analog telephone
A telephone that receives acoustic voice signals and sends analog electrical signals along the telephone line. Analog telephones are usually served by a single wire pair (tip and ring). The model-2500 telephone set is a typical example of an analog telephone.

ARS
See Automatic Route Selection (ARS) on page 392.

ART (Automatic Registration tool)
Tool used by services personnel to complete registration of an S8100 by requesting that alarming be turned on and tested.

ASCII (American Standard Code for Information Interchange)
The standard code for representing characters in digital form. Each character is represented by an 8-bit code (including parity bit).

Access Security Gateway (ASG)
A security management server that provides secure remote access to Avaya products installed at customer sites.

Audio Information Exchange (AUDIX)
A fully integrated voice-mail system. Can be used with a variety of communications systems to provide call-history data, such as subscriber identification and reason for redirection.

AUDIX
See Audio Information Exchange (AUDIX) on page 391.

Automatic Alternate Routing (AAR)
A feature that routes calls to other than the first-choice route when facilities are unavailable.

Automatic Route Selection (ARS)
A feature that allows the system to automatically choose the least-cost way to send a toll call.

B

bash (Bourne-again shell)
Unix-like command-line interpreter.

Basic Rate Interface (BRI)
A standard ISDN frame format that specifies the protocol used between two or more communications systems. BRI runs at 192 Mbps and provides two 64-kbps B channels (voice and data) and one 16-kbps D channel (signaling). The D channel connects, monitors, and disconnects every call. It also can carry low-speed packet data at 9.6 kbps.

C

cabinet
Housing for racks, shelves, or carriers that hold electronic equipment.

cable
Physical connection between two pieces of equipment (for example, data terminal and modem) or between a piece of equipment and a termination field.

cable connector
A jack (female) or plug (male) on the end of a cable. A cable connector connects wires on a cable to specific leads on telephone or data equipment.

call-accounting system (CAS)
This software feature provides recording, costing, and reporting of call detail records. Recording includes the capability to set record discard criteria that allow the customer to specify the data recorded. Costing uses tariff databases and user-defined parameters. Reporting produces both periodic reports for individual users, organizations, accounts, user-defined criteria, and demand statistics.

call-detail recording (CDR)
Textual representation of call traffic.

carrier
An enclosed shelf containing vertical slots that hold circuit packs.

CAS
See call-accounting system (CAS)

central office (CO)
The location housing telephone switching equipment that provides local telephone service and access to toll facilities for long-distance calling.

central office (CO) codes
The first three digits of a 7-digit public-network telephone number in the United States.

central office (CO) trunk
A telecommunications channel that provides access from the system to the public network through the local CO.

circuit
1. An arrangement of electrical elements through which electric current flows.
2. A channel or transmission path between two or more points.

circuit pack
A card on which electrical circuits are printed, and IC chips and electrical components are installed. A circuit pack is installed in a switch carrier.

CMC1
A cabinet formerly called a CMC (compact modular cabinet) which, when equipped with protocol-conversion hardware and software such as an S8100 Media Server, is a media gateway.

Communication Manager
The communication application that runs on Avaya servers to provide call control and telephony features. Formerly called MultiVantage software or Avaya Call Processing (ACP).

communications system
The software-controlled processor complex that interprets dialing pulses, tones, and keyboard characters and makes the proper connections both within the system and external to the system. The communications system itself consists of a digital computer, software, storage device, and carriers with special hardware to perform the connections. A communications system provides voice and data communications services, including access to public and private networks, for telephones and data terminals on a customer's premises. See also, switch on page 399.

compact modular cabinet (CMC)
See CMC1 on page 393 and media gateway on page 396.

The chassis and shelf hardware used to support an S8100's hardware platform, derived from (actually the same as) a DEFINITY ProLogix cabinet.

correlation ID
A temporary number that is created during the FET process. This number needs to be entered in RFA during the switch-configuration file's upload process.

CSA
Canadian Safety Association

D

digital
The representation of information by discrete steps. See also, analog on page 391.

digital trunk
A circuit that carries digital voice and/or digital data in a telecommunications channel.

E

E1
A digital transmission standard that carries traffic at 2.048 Mbps. The E1 facility is divided into 32 channels (DS0s) of 64-kbps information. Channel 0 is reserved for framing and synchronization information. A D channel occupies Channel 16.

F

FAC
Feature access code

FAS
Facility-associated signaling

Feature Extraction tool (FET)

FET is used for capturing customer features and settings for S8100 with G600 or CMC1 (DEFINITY ONE or IP600) R4 to R9 switches that cannot be contacted remotely. The output file from FET is used to create a license file for R10 or higher.

feature key words

These are used to identify RFA features.

G

G600

A cabinet formerly called an RMC (rack-mounted cabinet) which, when equipped with protocol-conversion hardware and software such as the S8100 Media Server, is a media gateway.

GAS

See Global Administration Subsystem (GAS)

GEDI

Graphically Enhanced DEFINITY interface. It is an enhanced system access terminal (SAT) with a Windows look.

Global Administration Subsystem (GAS)

A module that provides command-line access to certain administration and maintenance functions needed by services tools and provides administration support for parameters in the S8100 system that are not otherwise provided by the S8100 applications.

Global Alarm Module (GAM)

A Windows NT process that coordinates alarm reporting for the S8100 platform. Its primary functions are to accept and forward alarms from the applications, generate alarms for Windows NT, and manage the communication links to the Operations Support Systems (OSSs) via the Windows NT TAPI interface.

Global Sanity Keeper (GSK)

A module that ensures that every authorized Avaya application is executing on an S8100 server. It contains two major components, a watchdog process and a license server.

Glue application/module

An S8100 application that integrates functionality for most or all other S8100 applications. Examples include Watchdog, Lucent Access Control (LAC), Global Alarm Module (GAM), Global Administration Subsystem (GAS), and Backup/Restore.

graphical user interface (GUI)

The use of pictures rather than just words to represent the input and output of a program. A program with a GUI runs under some windowing system (for example, X Window System, Microsoft Windows, Acorn RISC OS, and NeXTstep). The program displays certain icons, buttons, dialogs, etc., in its windows on the screen and the user controls it mainly by moving a pointer on the screen (typically controlled by a mouse) and selecting certain objects by pressing buttons on the mouse while the pointer is pointing at them.

Group Authorization ID

Numbers assigned to a company or parts of a company. They are used to determine access permission to system records.

Integrated Services Digital Network (ISDN)
A public or private network that provides end-to-end digital communications for every service to which users have access by a limited set of standard multipurpose user-network interfaces defined by the CCITT. Through internationally accepted standard interfaces, ISDN provides digital circuit-switched or packet-switched communications within the network and links to other ISDNs to provide national and international digital communications. See also, Integrated Services Digital Network Basic Rate Interface (ISDN-BRI) and Integrated Services Digital Network Primary Rate Interface (ISDN-PRI).

Integrated Services Digital Network Basic Rate Interface (ISDN-BRI)
The interface between a communications system and terminal that includes two 64-kbps B channels for transmitting voice or data and one 16-kbps D channel for transmitting associated B-channel call control and out-of-band signaling information. ISDN-BRI also includes 48 kbps for transmitting framing and D-channel contention information, for a total interface speed of 192 kbps. ISDN-BRI serves ISDN terminals and digital terminals fitted with ISDN terminal adapters. See also, Integrated Services Digital Network (ISDN) and Integrated Services Digital Network Primary Rate Interface (ISDN-PRI).

Integrated Services Digital Network Primary Rate Interface (ISDN-PRI)
The interface between multiple communications systems that in North America includes 24 64-kbps channels, corresponding to the North American digital signal level-1 (DS1) standard rate of 1.544 Mbps. The most common arrangement of channels in ISDN-PRI is 23 64-kbps B channels for transmitting voice and data and 1 64-kbps D channel for transmitting associated B-channel call control and out-of-band signaling information. With nonfacility-associated signaling (NFAS), ISDN-PRI can include 24 B channels and no D channel. See also, Integrated Services Digital Network (ISDN) and Integrated Services Digital Network Basic Rate Interface (ISDN-BRI).

INTUITY AUDIX
The INTUITY AUDIX application resides on S8100 with the CornerStone platform to provide subscribers with messaging capabilities, including call-answering and voice-mailbox services.

IINTUITY Message Manager
A Windows-based software product that allows INTUITY AUDIX users to receive, store, and send their voice/fax messages from a PC. The software also enables users to create and send multimedia messages that include voice, fax, text, and file attachment components.

ISDN
See Integrated Services Digital Network (ISDN).

L

LAC
See Lucent Access Control (LAC) on page 396

LED
See light-emitting diode (LED) on page 396.

license file
Encrypted file that contains software category, release, feature and capacity RTUs, and the hardware serial number the license is tied to for a specific S8100.

License-Normal mode in DEFINITY
A license is properly installed and contains the correct serial number that matches the processor with purchased features (RTUs).

License-Error mode in DEFINITY
Call processing is supported, a major alarm has been declared and a 6-day shut-off timer is running. You must determine the cause of the inconsistency between the license and S8100, and fix it by obtaining and installing a valid license.

License Server
A component of the Global Sanity Keeper (GSK) that looks for a special encrypted control file whose contents indicate which serial number of the TN795 Processor card is permitted to execute on and which application are allowed to run. If the file is present, the license information is read from the file. If not, no licenses are granted.

light-emitting diode (LED)
A semiconductor device that produces light when voltage is applied. LEDs provide a visual indication of the operational status of hardware components, the results of maintenance tests, the alarm status of circuit packs, and the activation of telephone features.

local area network (LAN)
A networking arrangement designed for a limited geographical area. Generally, a LAN is limited in range to a maximum of 6.2 miles and provides high-speed carrier service with low error rates. Common configurations include daisy chain, star (including circuit-switched), ring, and bus.

Lucent Access Control (LAC)
A module that governs maintenance access to the Avaya application software.

M

maintenance
Activities involved in keeping a telecommunications system in proper working condition: the detection and isolation of software and hardware faults, and automatic and manual recovery from these faults.

maintenance update
This is a software update, the processor is not replaced.

major alarm
An indication of a failure that has caused critical degradation of service and requires immediate attention. Major alarms are automatically displayed on LEDs on the attendant console and maintenance or alarming circuit pack, logged to the alarm log, and reported to a remote maintenance facility, if applicable.

MAP-D
Multiapplication platform for DEFINITY.

media gateway
Hardware and firmware that converts between circuit-switched and packet-switched data. A CMC1 cabinet with an S8100 Media Server is the media gateway formerly called DEFINITY ONE. A G600 cabinet with an S8100 Media Server is the media gateway formerly called IP600.

media server
A processing platform running the Communication Manager, which provides call control and telephony features. The S8100 Media Server (which is implemented on the TN2314 circuit pack) can be housed in either the G600 or CMC1 cabinets.

memory
A device into which information can be copied and held, and from which information can later be obtained.

minor alarm
An indication of a failure that could affect customer service. Minor alarms are automatically displayed on LEDs on the attendant console and maintenance or alarming circuit pack, sent to the alarm log, and reported to a remote maintenance facility, if applicable.

modem
A device that converts digital data signals to analog signals for transmission over telephone circuits. The analog signals are converted back to the original digital data signals by another modem at the other end of the circuit. (MOdulator-DEModulator)

multileg cable, also called an octopus cable or a splitter cable
Processor interface cable.

N

NFAS
See Nonfacility-associated signaling (NFAS).

node
A switching or control point for a network. Nodes are either tandem (they receive signals and pass them on) or terminal (they originate or terminate a transmission path).

No-license error mode in DEFINITY
S8100 will run in Admin Mode only. You must determine the cause of inconsistency between the license and S8100 and obtain and install a valid license.

Nonfacility-associated signaling (NFAS)
A method that allows multiple T1 and/or E1 facilities to share a single D channel to form an ISDN-PRI. If D-channel backup is not used, one facility is configured with a D channel, and the other facilities that share the D channel are configured without D channels. If D-channel backup is used, two facilities are configured to have D channels (one D channel on each facility), and the other facilities that share the D channels are configured without D channels.

NT operating system
The Windows 32-bit operating system engineered by Microsoft. NT Servers provided centralized security, fault tolerance and additional connectivity while managing NT Workstations over a network.

O

Oryx API (OAPI)
Terminates the Oryx calls from the DEFINITY application and converts them to Windows NT primitives. Provides information through optical calls (for example, time of day and RYON board serial number) and supports the DEFINITY SAT interface.

OSS
Operations Support System.

OSSI
Operational Support System Interface.

P

Product Activation System (PAS)
The process of creating and installing license files, password files, ASG keys, Maestro records, and partial registration for S8100 with G600 or CMC1.

PCMCIA
Personal Computer Memory Card International Association.

PID
Product ID (also know as Alarm ID)

port
A data- or voice-transmission access point on a device that is used for communicating with other devices.

port network (PN)
A cabinet containing a TDM bus and packet bus to which the following components are connected: port circuit packs, one or two tone-clock circuit packs, a maintenance circuit pack, service circuit packs, and (optionally) up to four expansion interface (EI) circuit packs. Each PN is controlled either locally or remotely by a switch processing element (SPE).

port-network connectivity
The interconnection of port networks (PNs), regardless of whether the configuration uses direct or switched connectivity.

Primary Rate Interface (PRI)
A standard ISDN frame format that specifies the protocol used between two or more communications systems. PRI runs at 1.544 Mbps and, as used in North America, provides 23 64-kbps B channels (voice or data) and one 64-kbps D channel (signaling). The D channel is the 24th channel of the interface and contains multiplexed signaling information for the other 23 channels.

Processor Interface cable
Octopus cable, splitter cable, or multileg cable. See Install and cable a G600 cabinet on page 57.

processor port network (PPN) control carrier
A carrier containing the maintenance circuit pack, tone/clock circuit pack, and SPE circuit packs for a processor port network (PPN) and, optionally, port circuit packs.

Q

QPPCN
Quality Protection Plan Change Notice.

R

rack-mounted cabinet (RMC)
See G600 on page 394.

Remote Feature Activation (RFA)
The web-based system that is used to deploy license and password files for every DEFINITY platform.

remote maintenance board (RMB)
A board provided in adjunct processors that intelligently monitors the system hardware for health status. These include environmental conditions, PC heartbeat, and sanity checks. The RMB functionality also allows modem access to the TN parent board.

RS-232C
A physical interface specified by the Electronic Industries Association (EIA). RS-232C transmits and receives asynchronous data at speeds of up to 19.2 kbps over cable distances of up to 50 feet.

RTU
Right-to-use fee that is charged for feature activation.

S

S8100 Media Server
The Avaya S8100 Media Server is an application-enabling processing platform that runs Avaya Communication Manager and is supported in the Avaya G600 and CMC1 Media Gateways.

Sanity Keeper
See Global Sanity Keeper (GSK) on page 394.

SAP
Avaya's ordering system for products and services.

serial number swap-outs
There is an RFA process to update the system record and issue a new license file when hardware is swapped out. You must have a valid license file installed, because it must match the information on the new processor.

SID
System identification number provided when a system record is created by RFA. This number is unique and static.

single-carrier cabinet
A combined cabinet and carrier unit that contains one carrier. See also, multileg cable, also called an octopus cable or a splitter cable on page 397.

Station Message Detail Recording (SMDR)
This software feature transmits detailed information about every incoming and outgoing call on specified trunk groups through a switch processing element (SPE) port to an external output device, that logs the data. SMDR is one facet of the more general call-detail recording (CDR) capability.

switch
Any kind of telephone switching system. See also, communications system on page 393.

switch-processing element (SPE)
A complex of circuit packs (processor, memory, disk controller, and bus-interface cards) mounted in a PPN control carrier. The SPE serves as the control element for that PPN and, optionally, for one or more EPNs.

system administrator
The person who maintains overall customer responsibility for system administration. Generally, every administration function is performed from the Management Terminal. The switch requires a special login, referred to as the system administrator login, to gain access to system-administration capabilities.

system record
RFA record for each licensed S8100.

T

TCP/IP
Transmission Control Protocol/Internet Protocol

troubleshooting license
License created when troubleshooting requires some features to be activated or deactivated. This is only accessible by Avaya's Tier-3 and -4 personnel.

U

UL
Underwriters' Laboratories, Inc.

update
A modification to a release of software, such as applying patches to an S8100 system.

upgrade
Replacement of an existing system-software release with a later release.

URL
uniform resource locator

V

Virtual Fabric Manager (VFM)
A module that allows Communication Manager's code to operate in a different hardware environment from its native environment. One side of the VFM talks to Communication Manager in protocols it understands and changes these into methods and messages to perform needed operations in the S8100 environment.

W

Watchdog
A component of the Global Sanity Keeper (GSK) that is responsible for starting up the S8100 application software, including the downloading of the MPC860 application firmware. Watchdog is the first S8100 process to run.

Index

Symbols

µ-Law companding, 181

Numerics

120A2 integrated channel-service unit, 105
25-pair cable pinout, 129
26B1 selector console, 109
3- and 4-pair modularity, 105
302C1 attendant consoles, 99
367A adapter, 120

A

AC
  load center, 72, 357
  power
    checking, 72, 357
    ground wiring, 75, 360
    supply, 72, 357
  voltage test, 72, 357
access methods, 151
  Telnet session, 152
  Web browser, 153
adapter, BR851-B, 119
adding
  circuit packs, 229, 243
  C-LAN functionality, 230
  CO trunk, 236
  code calling access, 239
  DID trunk, 236
  DS1 service interruption, 238
  FX trunk, 236
  ISDN-PRI, 242
  PCOL trunk, 236
  remote machines, 216
  speech synthesis, 239
  switch configuration, 253
  tie trunk, 237
  TN2464BP, 234
  TN464GP, 234
  translations, 181
  voice-mail item, 254
  WATS trunk, 236
address, setting RAS IP, 333
adjunct power
  connection, 106
  providing, 100
administering
  AUDIX, 194
  customer's LAN parameters, 163
  DEFINITY for AUDIX initialization, 185
  digital networking, 207
  modem, 262
  no-license/emergency number, 171
  S8100, 174
  SNMP, 199
  telephone features, 182
alarm
  checking, 172
  connections, 113
  input, 113
  origination disable procedure, 262
  output, 113
  relay contact, 113
  resolve, 173
alarmstat bash command, 173
A-Law companding, 181
announcements
  CWY1, 240
  moving, 240
  multiple integrated recorded announcements, 239
  TN750C circuit pack, 240
APP connector information, 99, 270, 278, 281 to 283
approved grounds, 73, 75, 358, 360
ART
  download installation script, 166
  URL, 166
ASA
  launching emulation session, 255
  launching voice-mail administration session, 256
attendant console, 181
  302C1, 99
  LEDs, 325
  maximum cabling distance, 99
AUDIX
  adding subscribers, 194
  administration, 194
AUDIX initialization
  check dial plan, 185
  checking
    class of service, 186
    dial plan, 185
    hunt groups, 186
  class of restriction, 187
  class of service, 187
  coverage plan, 193
  dial plan, 188
  hunt groups, 191
  test phone adding, 193

auxiliary
  equipment
    pin designations, 281 to 283
    pinout information, 99, 270, 280 to 283
  power, 115
Avaya Site Administration
  adding
    new switch configuration, 253
    new voice-mail item, 254
  components, 249
  configuring, 253
  download, 197
  hardware configuration, 248
  help, 251
  help system, 248
  launching GEDI session, 254
  overview, 245
  starting sessions, 199
  switches, 248
  tasks, 251
  version 1.5 features, 247
  voice mail, 248
  Windows 95/98 configuration, 249

B

backups
  adding a scheduled backup, 205
  procedures, 302
  scheduling, 205
  Web interface, 305
bash commands, listed, 329
bit rate, setting, 269
BR851-B adapter, 119
BRI
  multipoint cabling distances, 121
  terminating resistor, 116
building steel, as approved ground, 73, 358
button labels
  printing, 251
  printing, in ASA, 247
  templates, 251

C

cabinets
  cabling, 57, 343
  cross connecting to MDF, 372
  cross-connecting to MDF, 86
  floor mounting, 350
  installing, 57, 343, 352
  numbering, 91, 378
  plywood backing, installing, 351
  power switches, 74
  single-cabinet installation, 351
  two horizontally mounted cabinets, 351
  two vertically mounted cabinets, 351
  wall mounting, 350
cables
  25-pair pinout, 129
  diagrams, 99, 270, 278, 281 to 283
  pinouts, 267
cabling the cabinet, 57, 343
call accounting, 185
call-detail recording (CDR)
  mapping shared directory, 183
  setting call collection interface, 184
  setting up, 182
  sharing data, 183
  verifying call record collection, 184
call-progress tones, setting up country-specific, 176
carrier address ID, setting, 65, 348
CD-ROM
  mapping S8100 to laptop's CD-ROM, 144
  sharing laptop's CD-ROM drive, 144
change INTUITY AUDIX commands
  change machine, 212
  change system-parameter limits, 210
changing
  system-parameters country options, 180
channel-service units (CSUs), 105
checking
  AC power, 72, 357
  alarms, 172
  customer's order, 59, 343
  system's status, 173, 180
checklists
  for installation technicians, 5
  to install and cable cabinet, 5
circuit modules, 86
  disallowed, 89, 375
circuit packs, 86, 372
  adding, 229, 243
  allowed, 86
    for CMC1, 372
    for G600, 86
  disallowed, 89, 375
    for CMC1, 375
    for G600, 89
  downloading firmware, 227
  installation, 91, 377
  LEDs, 325
  pin designations, 281 to 283
  slot loading, 91, 377
  status LEDs, 326
  TN2185 ISDN-BRI 4-wire S Interface, 277
  TN2224 Digital Line, 274, 280
  TN725B speech synthesizer, 239
  TN744D call classifier/tone detector, 377
  TN750C announcement, 239, 240
  TN795 processor, 91, 226, 377
circuit protection
  off premises, 93, 380
  protectors, 124
C-LAN functionality, 230
CMC1
  allowed circuit packs, 372
  disallowed circuit packs, 375
CMC1 cabinets
  power switches, 359

CMC1 installation
cabinets, cross connecting to MDF, 372
carrier address ID, 348
circuit packs
allowed, 372
disallowed, 375
comcodes for CMC1 equipment, 345
connecting and routing power cords, 364, 401
coupled bonding conductor, 364
equipment-room hardware
CMC1 equipment-room hardware, 372
floor mount cabinet, 350
main distribution frame and external modem, 370
MDF, labling, 383
off-premises circuit protection, 380
power switches, cabinet, 359
setting ringing option, 385
system cabinet, 348
unpack equipment, 344
wall mount cabinet, 350
CO trunk, adding, 236
code calling access, adding, 239
cold starts with translations, 320
comcodes, equipment packed with
CMC1, 345
G600, 63
commands
bash
alarmstat, 173
d1backup, 304
d1disable snmp, 178
d1enable snmp, 178
d1stat, 173
ftpserv, 334
net user, 290, 335
reboot, 295, 317, 332, 334
serialnumber, 163
setip, 152, 164, 295, 332, 333, 334
shutdown, 318
statapp, 334
swversion, 163
categories, 293
DEFINITY, for user, 293
installconfig, 261
INTUITY AUDIX, 194
change machine, 212
change machine remote_machine_name, 219
change system-parameter limits, 210
LAC, 331
LAC bash, 329
commercial AC power, 72, 357
companding, 181
companding modes, 180
concrete-encased ground, 73, 358
configuring
Avaya Site Administration, 253
customer's LAN, 149
servers, DHCP and TFTP, 161
switches, 253
connecting
AC power, 72, 357
laptop computer, 140
management terminal, 99
power cords, 78, 364, 401
telephones, 99
connection icon, creating, 150
connections
keyboard, 149
LAN, 149
modem, 149
monitor, 149
mouse, 149
connectivity and access
S8100, 139
copy protection, 265
country codes
listed, 179
setting, 179
country options, setting, 179, 180
coupled bonding conductor, 76, 77, 78, 362, 364
creating DEFINITY ONE connection icon, 150
customer's
access, 285
LAN, configuring, 149
order, checking, 59, 343
CWY1 announcements, 240

D

D1 bash commands
d1backup, 304
d1disable snmp, 178
d1enable snmp, 178
d1stat, 173
date and time
S8100, remote dial-in, 175
S8100, using CLI, 175
S8100, using terminal server, 174
setting, 174
DC power, signaling leads, 267
defragmenting, using Diskeeper, 315
deleting nonadministered remote users, 223
DHCP server, configuring, 161
digital networking
adding remote machines, 216
administering networking channels, 211
changing local machine information, 212
changing local machine profiles, 212
completing remote machine profiles, 219
completing the Digital Machine Administration window, 217
feature options, 209
full remote update, 223
initial administration, 207
initial tasks, 208
local machine information, 212
networking channels, 211
number of users, 210
remote extensions, 224
remote machine profiles, 219
remote users, 210
verifying purchased options, 209

digital tie trunk, 103
Diskeeper defragmentation software, 315
disks, see hard disks
DNS, setting customer's information, 333
drives, see hard disks
DS1
  adding service interruption, 238
  tie trunk, 105

E

echo cancellation
  with TN2464BP, 234
  with TN464GP, 234
electrical connection, 72, 357
embedded messaging
  enable/disable, 314
  maintenance impact, 314
emergency transfer
  power panel, 115, 127
  telephone, 133, 401
emulation sessions, launching, 255
enable/disable embedded messaging, 314
equipment
  checking, 59, 343
  checklist, 140
  comcodes for CMC1 equipment, 345
  comcodes for G600 equipment, 63
  unpacking, 60
  unpacking CMC1, 344
equipment-room hardware, installing, 86
error messages, by installation wizard, 259
external modem
  connecting, 135
  installing, 85, 371
  option settings, 85, 135, 371
  type-approved, 85, 371
  US Robotics, 85, 135, 371

F

faceplates
  TN2314 Processor circuit pack, 323
  TN795 Processor circuit pack, 98, 386
Feature Extraction tool, 165, 225
feature protection, 265
FET, 165, 225
firmware
  downloading, 227
floor grounds, 74, 358
floor-mounted cabinet, 350
ftpserv bash command, 334
FX trunk, adding, 236

G

G600 installation, 58
  AC power and ground, 72
  cabinet's power switches, 74
  cabinets, cross-connecting to MDF, 86
  circuit packs
    allowed, 86
    disallowed, 89
  connect power cords, 78
  coupled bonding conductors, 78
  disallowed circuit packs, 89
  equipment-room hardware, 86
  off-premises circuit protection, 93
  setting ringing option, 97
  system cabinet, 65
GAS commands, 329
GEDI launching sessions, 254
ground blocks
  installation to right panel, 361
  installing, 360
ground rings, 73, 358
ground wiring, AC, 75, 360
grounds
  approved, 73, 75, 358, 360
  approved floor, 74, 358
  building steel, 73, 358
  checking, 72, 357
  concrete-encased, 73, 358
  connecting, 75, 360
  single-point, 75, 360
  water pipes, 73, 358

H

hard disks
  identifying for QP1413b, 387
  replacing, 226
hardware
  additions, 229
    circuit packs, 229
    CO, FX, WATS, and PCOL, 236
    code calling, 239
    DID trunks, 236
    IP trunk, 230
    speech synthesizer circuit pack, 239
    tie trunks, 237
    TN750C circuit pack, 239
  configuration, for Avaya Site Administration, 248
help, online for Avaya Site Administration, 251
horizontally mounted cabinets, 351
hunt groups, 186, 191

I

identifying, hard disks for QP1413b, 387
impedance, setting, 269
INADS modem, 262
initializing the system, 159
install and cable cabinet, checklist, 5
installation
  BRI terminating resistor, 116
  checklists, 5
  circuit packs, 91, 377
  coupled bonding conductors, 78, 364
  emergency transfer power panel, 127
  equipment-room hardware, 86
  error messages, 259
  external modem, 85, 371
  G600, 58
  ground block, 360
  Intuity AUDIX languages, 299, 301
  main distribution frame and external modem, 370
  Message Manager, 197
  multipoint adapters, 119
  off-premises station wiring, 122
  password file, 168
  S8100, 58
  script, 168
    download from ART, 166
    install, 169
    manual installation, 170
  sneak fuse panels, 94, 381
  system cabinet, 65, 348
  telephones, 99
installconfig command, 261
Installing INTUITY AUDIX languages, 299
installing the cabinet, 57, 343
integrated channel-service unit (ICSU), 105
INTUITY AUDIX
  commands, 194
  Communication Manager administration, 185
  digital networking, 207
  languages, installation, 299, 301
  networking, 207
IP solutions, Media Processor, 233
IP trunks, installing, 230
IP, setting RAS IP address, 333
IP600 installation
  unpacking, 60
ISDN-BRI
  fanout of multipoint installations, 121
  terminating resistor, 116
ISDN-PRI, adding, 242

L

label main distribution frames, 383
LAC bash commands, listed, 329
LAN
  IP Trunk, 230
  setting customer's information, 333
laptop computer
  connecting, 140
lead designations, 270
  port boards, 115
  telephones, 115
LEDs, 162
  alarms, 322
  attendant console, 325
  boot sequence, 321
  circuit packs, 325
  on Maintenance/Processor circuit packs, 322
  power supply, 327
  TN2314 Processor circuit packs, 322
local machines, changing information, 212
login groups, 286
login names, 286
logins
  for customer, 173
    as
      administrator, 286
      super-user, 292
    to
      INTUITY AUDIX, 174, 287
      Web, 174, 288
      Windows, 286
      Windows NT, 290
  versus command permissions
    in INTUITY AUDIX, 287
    setting up, 292
Lucent access controller (LAC) commands, 329

M

machine name, setting in Windows, 332
main distribution frames
  installing external modem, 370
  labeling, 383
major-alarm contact, 113
mapping
  drives, during upgrades, 299
  Map Network Drive wizard, 342
  S8100 to laptop's CD-ROM, 144
  shared CDR directory, 183
material stocking location (MSL), see National Parts
MDF
  cross-connecting cabinet, 86, 372
  mounting, 370
measurements, security, 292
Message Manager
  downloading, 257
  installing, 197
  introduction, 257
modem
  administration, 262
  external, switch settings, 85, 135, 371
  INADS, 262
  installing external, 85, 371
  setup, 262
modularity
  3-pair, 105
  4-pair, 105

mounting MDFs, 370
mu-Law companding, 181
multiple cabinets
  cabling, 57, 343
  installing, 57, 343
multipoint adapters
  figure, 121
  installation, 119

N

name, setting machine name in Windows, 332
National Electrical Code (NEC) grounding rules, 72, 357
National Parts, 59, 344
neon voltage, versus ring ping, 136
net user bash command, 290, 335
NETBUI, and mapping drives, 299
networking channels, digital networking, 211
no-license/emergency numbers
  administer, 171
nonadministered remote users, deleting, 223
NT1 network interface, 116

O

off-premises
  circuit protection, 93, 380
  stations, 122

P

password file
  installing, 168
  transfer, 168
PCOL trunk, adding, 236
pedestal, for floor-mounted CMC1, 350
pin designations
  auxiliary equipment, 281 to 283
  circuit packs, 281 to 283
pinout information
  auxiliary equipment, 99, 270, 280 to 283
  cables, 267
  circuit packs, 99, 270, 281 to 283
    port packs, 115
    TN2185 ISDN-BRI, 277
    TN793 Analog line, 278
  connector and cable diagrams, 270
  Processor Interface cable, 274
  telephones, 115
port circuit pack, pinout information, 115
power
  cords
    connecting, 78, 364, 401
    routing, 78, 364, 401
  holdover, 74, 359
  supply
    LEDs, 327
    uninterruptible, 74, 359
  switches
    cabinet, 74
    CMC1, 359
procedures, backup, 302
Processor Interface cable
  connection, 79, 113, 367
  pinout, 274
Product-ID, setting, 171
progress tones, setting up country-specific, 176

Q

QP1413b, identifying correct hard disks, 387

R

R300 Remote Office Communicator, 230
RAS, setting IP address, 170, 333
reboot bash command, 295, 317, 332, 334
recovery, of system, 317
remote machines
  adding digital networking, 216
  completing profiles, 219
remote office
  adding, 230
  Avaya R300 Remote Office Communicator, 233
remote users digital networking, 210
replacing
  hard disk, 226
  TN795 with a TN2314, 225
resets
  reset system 3, 320
  reset system 5, 320
RFA
  overview, 164
ringing
  preventing ring ping, 136
  setting ringing option, 97, 385
routing power cords, 78, 364, 401

S

S8100
  accessing, 151
  connectivity and access, 139
  installation, 58
  shutdown, restart, 317

safety precautions, 52
SAT session, connecting via Telnet, 296
scheduling
  backups, 205
  Diskeeper defragmentation, 315
security measurements
  forced password aging, 292
  logoff notification, 292
selector consoles, 26B1, 109
setip bash command, 152, 164, 295, 332, 333, 334
setting
  bit rate, 269
  carrier address ID, 65, 348
  country-specific call-progress tones, 176
  date and time, 174
  line impedance, 269
  RAS IP address, 333
  ringing option, 97, 385
  switch name, 295
settings
  displaying current settings, 332
  LAN, DNS, WINS, 333
shipping errors, correcting, 59, 344
shutdown bash command, 318
signaling leads, DC power, 267
single-point
  ground block, 75, 360
  grounds, 75, 360
site requirements, 58
slot loading of circuit packs, 91, 377
slot numbering, 91, 378
sneak current
  fuse panels, 94, 381
  fuses, 95, 382
  protection, 94, 381
sneak fuse, connector pinout, 95, 382
SNMP
  administering, 199
  community string configuration, 202
  disable, 178
  enable, 178
  starting and stopping, 203
  trap destination configuration, 200
software
  copy-protection mechanisms, 265
  recovery, 319
  serial number serialnumber bash command, 163
  version, 163
speech synthesis, adding, 239
statapp bash command, 334
stations connections, 102
status
  checking system's status, 173, 180
  LEDs on circuit packs, 326
super_user, 292
switch name, setting, 295
switch settings
  external modem, 85, 135, 371
  TN464 circuit pack, 269
  TN760 tie trunk, 267
switches
  adding new switch configuration, 253
  interacting with Avaya Site Administration, 248
swversion bash command, 163
system
  cabinet, installing, 65, 348
  initialization, 159
  reboots, 320
  recovery, 317
  resets, reasons for, 319

T

T1 channel-service unit, 105
telephone
  connection, 99
  emergency transfer, 133, 401
  features, administering, 182
  installing, 99
  pin designations, 115
  pinout information, 115
Telnet session, 152
templates, for
  adding objects, in ASA, 250
  button labels, in ASA, 251
  rack-mounted G600, 6, 65
  wall-mounted CMC1, 352
terminal connections, 99
terminating resistor, 116
  adapter, 116
  block, 117
test call, 182
TFTP server, configuring, 161
tie trunk
  adding, 237
  circuit pack option settings, 267
  connectivity, 104
  digital wiring, 103
time, setting, 174
TN2181, pinout information, 115
TN2224 Digital Line, 274, 280
TN2314
  faceplate, 323
  LEDs, 322
  replacing a TN795, 225
TN2793, 278
TN464, option settings, 269
TN750C, 240
TN760, option settings, 267
TN793, 278
TN795
  faceplate, 98, 386
  replace the circuit pack, 226
  replacing with a TN2314, 225
TN799C, installing, 231
transfer password file, 168
translations
  adding, 181
  copy protection, 265
  save procedure, 99
troubleshooting, 259
  commands, 261
  error messages, 259
trunks, adding, 236
type-approved external modem, 85, 135, 371

U

uninterruptible power supply (UPS), 74, 359
unpacking
  CMC1, 344
  equipment, 60
upgrade
  hardware, 229
  to a TN2314, 225
UPS, 74, 359
US Robotics modem, 85, 135, 371

V

vertically mounted cabinets, 351
voice mail
  adding items, 254
  interacting with Avaya Site Administration, 248
  launching administration session, 256

W

wall-mounted cabinets, 350, 351, 352
waterpipes, as approved ground, 73, 358
WATS trunk, adding, 236
Web
  browser, accessing S8100, 153
  logins, 174
Windows logins, 290
WINS, setting customer's information, 333
wiring
  analog tie trunk, 103
  color code, 102
  digital tie trunk, 103
  examples
    3- and 4-pair modularity, 105
    302C attendant console, 99
    analog tie trunk, 103
    attendant console, 99
    digital tie trunk, 103
    telephone connection, 99
  pin designations, 281 to 283
  pinouts, 99, 270, 278
  Processor Interface cable, 79, 86, 113, 367, 371
  telephone connection, 99
wizards, Map Network Drive, 342
www.messenger, 257